8-2015

Analytics and Cybersecurity: The Shape of Things to Come

Gary PAN
Singapore Management University, garypan@smu.edu.sg

Poh Sun SEOW
Singapore Management University, psseow@smu.edu.sg

Calvin CHAN

Chu Yeong LIM
Singapore Management University, cylim@smu.edu.sg

Analytics and Cybersecurity: The shape of things to come

Edited by Gary Pan, Seow Poh Sun, Calvin Chan and Lim Chu Yeong

CPA AUSTRALIA

SMU
SINGAPORE MANAGEMENT UNIVERSITY

SIM UNIVERSITY

Analytics and Cybersecurity: The shape of things to come

Gary Pan, Seow Poh Sun, Calvin Chan and Lim Chu Yeong
Editors

First published August 2015

Analytics and Cybersecurity: The shape of things to come

Editors : Gary Pan, Seow Poh Sun, Calvin Chan and Lim Chu Yeong

Published by : CPA Australia Ltd
1 Raffles Place
#31-01 One Raffles Place
Singapore 048616

Website : cpaaustralia.com.au

Email : sg@cpaaustralia.com.au

ISBN : 978-981-09-5560-1

TABLE OF CONTENTS

FOREWORD

Analytics and data are said to underpin Singapore's development towards a Smart Nation. For companies, being able to effectively analyse and make sense of the avalanche of data is fundamental to predicting what will happen next in order to make smarter decisions and improve business outcomes. Experts believe that data and analytics provide enormous opportunities to help companies expand their business, reduce costs, increase efficiency, improve quality, and facilitate the greater participation in global commerce.

With the new Internet of Things (IoT) phenomenon expected to grow quickly, it will be more challenging for companies to deal with the massive amounts of structured and unstructured data that will come to light. But as companies accumulate an increasing mountain of data in the course of business, they face increasing risks of the information landing in the wrong hands, such as through internal leaks and cyber attacks by hackers.

Cybersecurity has grabbed headlines in recent years with several high profile cases locally and globally. A hacker attack in late 2014 on Sony Pictures Entertainment resulted in emails and files of unreleased Sony films being leaked. In October 2014, reports surfaced that hackers had breached the accounts of more than 70 million customers of the lender JPMorgan Chase. In Singapore, nearly 1,600 SingPass accounts were accessed illegally in June 2014, while in September, hackers leaked details of more than 300,000 customers of the karaoke chain Kbox. Since 2013, there has also been a string of hacking incidents on Singapore government websites, including that of the Prime Minister's Office.

Governments are now paying more attention to this developing phenomenon. Singapore, for instance, has set up a Cyber Security Agency and appointed a cabinet minister to be in charge of cyber security.

Against this backdrop, our three organisations believe there is merit in contributing to the eco-system by equipping corporate decision makers with the necessary insights to understand the hottest issues relating to analytics and cybersecurity. With this in mind, we have invited contributions from industry and academia to bring together the thought leaders in the critical issues of analytics and cybersecurity. Their inputs have resulted in this toolkit aimed at directors and senior management in corporates and SMEs, as well as business advisors at large. We are grateful for the contributions of DBS, Deloitte, EY, KPMG, PwC as well as colleagues from our two participating universities in this publication. We hope you will find this to be a useful resource for your business.

Philip Yuen FCPA (Aust.)
Divisional President
– Singapore,
CPA Australia

Prof Cheng Qiang
Professor of Accounting
and Dean, School of
Accountancy, Singapore
Management University

Assoc Prof Lee Pui Mun
Associate Professor and
Dean, School of Business,
SIM University

August 2015

PROLOGUE

As global marketplace becomes increasingly complex, analytics may provide enterprises with important capabilities to derive insights from data. This may help enterprises to make more effective and timely decisions and allow them to create a competitive edge for themselves. With several on-going public and private sector initiatives on analytics, the high level of interest in analytics is clearly evident in Singapore. The interest in analytics may have gathered momentum after Singapore announced its vision to transform itself into a Smart Nation that is underpinned by data and analytics.

While data and analytics are crucial in developing a Smart Nation, one must not forget the importance of protecting IT infrastructure. Major challenges relating to cybersecurity include how to securely authenticate who is coming into the network and identification of anomalies occurring in enterprises' networks in real time.

Enterprises may need to optimise their data collection and analytics efforts to detect and defend against cyber intrusions. As cybersecurity challenges continue to grow, with new threats expanding exponentially and with greater sophistication, enterprises may have to increase their understanding of readiness and vulnerabilities — as well as their views on big data cybersecurity analytics — versus reality.

As editors of this book, we brought together authors to answer important questions such as what are analytics and cybersecurity and why are they important? How do you implement analytics and cybersecurity? Whom and what important implementation lessons we can learn from? Our objective is to bring forth issues in academic and professional literature on analytics and cybersecurity for further study and discussion.

This book is organised as follows.

Chapters 1-6 focus on 'ABCs of Analytics'. **In Chapter 1**, you will learn that there is increasingly a shift in mind-set towards data driven decision making in accounting departments. Accountants may move beyond optimising accounting function to transforming the enterprise, particularly in areas such as internal audit, external audit and, risk and fraud detection.

Chapter 2 highlights the importance of proper planning and executing analytics projects. It proposes an Aspect-Oriented Business Analytics Framework that emphasises critical aspects such as business, data and analytics that should be considered when planning business analytics and big data initiatives.

Chapter 3 describes key elements of analytics led transformation journey for Finance, along with a few simplified illustrative examples of how Finance can use analytics to partner Business to identify potential areas of value creation.

In **Chapter 4**, you will learn that a data-focused approach may allow Internal Audit functions to identify issues, target risks and allocate resources more effectively. Enterprises should consider a more real-time and end-to-end data driven Internal Audit model that may allow them to move from simply auditing around historic risks to monitoring and pivoting based upon prospective risks.

Chapter 5 explores how risk analytics may be a critical capability in developing and sustaining a competitive edge especially at a time when risk issues affect business strategy more than ever.

Chapter 6 examines how forensic data analysis may provide the ability to comprehensively look through large data sets and spot unusual patterns or anomalies that are otherwise invisible. This may enhance fraud detection activity as enterprises can do more in managing fraud risks through such effective anti-fraud technique.

Chapters 7-12 describe how organisations may formulate their cybersecurity strategy. In **Chapter 7**, you will learn that business managers and executives need to play a larger and more direct role in managing cybersecurity. The chapter introduces various cybersecurity concepts and offers a conceptual framework on cybersecurity strategy.

Chapter 8 advocates an appropriate cyber risk management programme should be one of many components of the organisation's IT governance process that covers the overall business risk environment that feeds into its enterprise-risk management framework.

Chapter 9 highlights analytics may allow organisations to derive deeper intelligence from their data-sets. When applied to cybersecurity, the actionable insights provided should allow them to detect and stop potential breaches faster and more efficiently.

Chapter 10 raises an important issue of adopting a risk-initiated approach to anticipate as much as possible the scenarios in which a cybersecurity breach might occur. Enterprise ought to strive to reduce the time lapse between the breach and detection to limit the potential damage arising from a successful attack.

Chapter 11 highlights cybersecurity is becoming a top-of-mind issue for most boards, and directors are becoming more pre-emptive in evaluating cybersecurity risk exposure as an enterprise-wide risk management issue and not limiting it to an IT concern.

Chapter 12 points out that cyber crimes and attacks are becoming increasingly common and enterprises should be prepared to detect and respond to cyber incidents when they happen. It is vital for enterprises to understand digital forensic principles and procedures that may aid investigations, as well as enable a better understanding of threats faced.

We are pleased to be a small part of this collaboration between CPA Australia, SMU School of Accountancy and SIM University. We thank the contributing authors for their support in this project. We hope you, the readers, find this collection of articles thought-provoking and useful in your pursuit of analytics and cybersecurity.

Gary Pan FCPA (Aust.), Seow Poh Sun FCPA (Aust.) and
Lim Chu Yeong CPA (Aust.)
Singapore Management University

Calvin Chan
SIM University

Part 1
The ABCs of Analytics

CHAPTER 1

FROM DATA ANALYSIS TO INTELLIGENT ACCOUNTING: IMPACT OF ANALYTICS ON ACCOUNTING FUNCTION

Gary Pan and Seow Poh Sun, Singapore Management University

Background

In May 2011, an article published in MIT Technology Review suggested effective data analysis might create new business opportunities as technologies were converging to offer companies more power to detect what their users might want (Gomes, 2011). It is obvious that data analysis is not a new concept, in fact, it's been around for decades. Interestingly in the last two to three years, we have seen many companies asking what is analytics and why the hype. Whether it is data analysis, data analytics or business analytics, the truth of the matter is that analytics is getting a lot of attention. So if data analytics is not new, why is analytics so big now? There are three main reasons: Advancement of analytical tools; abundance of structured and unstructured data; and increasing dominance of a data-driven mind-set.

With the availability of advanced analytical tools and technologies, analytics allows business executives to seek timely and relevant data, which enables them to make better business decisions, grow revenue, maximise organisational efficiencies, and manage risk and compliance. The advancement in analytical tools certainly plays a key role in supporting data visualisation, statistical analysis and text mining among other capabilities.

In terms of data availability, companies typically focus on data that are stored in a structured form (e.g., spreadsheets, databases and so on) that can be queried using structured query language. While the analyses on structured data offer significant insights, they apparently cover only 20 per cent of the data held on company computer systems. Approximately 80 per cent of the company's data are stored in an unstructured form which does not lend itself to conventional analysis. These unstructured data may include employees' electronic mails, telephone conversations and many others.

So with substantial untapped unstructured data, the major decision lies in whether to allocate resources to mine unstructured data in order to analyse patterns of behaviour and establish relevant links between individuals and activities to extract valuable insights into business activity. With the availability of advanced analytical applications today to keep pace with increasing data volumes, as well as business and regulatory complexities, the most effective analytical strategy may be to integrate available structured and unstructured data, and then perform data analytics that will help gain deeper business insights. For instance, one may leverage data from electronic mail conversations and social media sites, and combine insights gained from these (unstructured) sources with official (structured) records and transactions in traditional databases and spreadsheets. In other words, integrate social media, electronic mail, free-text and other unstructured data sources into traditional analyses that historically rely on only numerical information. The mining and visual analytical tools would help to highlight anomalies derived from the multi-dimensional attributes within the dataset.

Most importantly, there is increasingly a shift in mind-set towards data driven decision making especially in accounting departments. Analytics is a way to glean deeper insights into the internal and external forces that influence the company's performance. With data-driven decision making culture, there is opportunity for accountants to move beyond optimising the accounting function to transforming the enterprise. For instance, by analysing deeper into performance metrics such as resource productivity, debt recovery and inventory turnover, accountants may gain insights to their businesses and integrate business processes as part of a broader enterprise transformation. Analytics has impacted accounting activities in several major areas such as internal audit, external audit and, risk and fraud detection.

Internal audit

Typically, the role of an internal audit function is to identify fraud, improve processes and control-monitoring, and promote policy compliance. In particular, internal audit has an important role to play in fraud prevention. This is especially so when fraud has been a persistent threat for Singapore companies, affecting more than one in four companies in Singapore. To make matters worse, the frequency of fraud occurrence continues to rise over the past few years. The KPMG-SMU 2014 Singapore Fraud Survey reports that 29 per cent of the survey respondents indicated at least one fraud incident had occurred in their organisations as compared to 22 per cent in the 2011 survey. The survey also finds that internal fraud has risen since 2011 and remains the most significant threat. 58 per cent of the fraud incidents reported in 2014 were perpetrated by employees as compared to 47 per cent in 2011.

Major organisations have begun to carry out continuous auditing across the organisation so as to minimise operational risks and costs, and optimise efficiency. Continuous auditing is the collection of audit evidence and indicators by an internal auditor on processes, transactions, and controls on a frequent basis (Miklos and Chan, 2011). Internal audit capability is enhanced by analytics in the following ways: automation of risk monitoring activity; auditing a full data population, rather than sampling, and analysing data patterns across multiple transaction processing systems; and continuous monitoring for policy infringements. An example of continuous auditing activity is the assessment of controls around vendor setup to prevent payment to fictitious vendors by focusing on the potential of authorised users performing unauthorised business activities.

Overall, analytics contributes to internal audit activities in the following ways: (1) ability to analyse 100 per cent of the data at a much shorter time as compared to manual review; (2) real time red flags can be identified with the use of continuous monitoring; (3) range of exposure can be broadened and the ability to uncover new patterns of fraudulent behaviour is increased. Data analytics has become more predictive and could enhance fraud prevention activities; and (4) reduce unnecessary cost by identifying inefficient and ineffective business activities.

External audit

Large public accounting firms typically focus on the impact that data analytics will have on how external audits are planned and conducted in key business processes, including order-to-cash, procurement-to-pay, inventories, fixed assets, journal entries and etc. An advantage for using analytics is that as the auditing environment and standards have become increasingly complex and demanding, this implies more effort and hours will have to be invested when conducting audits. A well-implemented audit plan with embedded data analytics could minimise the hours and improve overall efficiency. For example, analytics tools extract data from tables in organisations' enterprise resource planning systems. Data are processed using a list of routines that analyse the entire population. Analytics supplement or even replace much of the manual test work performed, and hence allow auditors to use the incremental capacity on other key risk areas. Furthermore, audit firms are increasingly expected to provide thought leadership and industry expertise. As a result, analytics may be a useful tool to analyse organisations' performance data in greater depth which may produce fresh ideas or new perspectives.

Auditors are also increasingly using data analytics to conduct journal entry testing. Financial statement frauds often involve fraudulent manual journal entries such as back-posting journal entries, hiding/obscuring entries, manipulating earnings, reserves and revenue, quarter-to-quarter timing issues, and subverting approvals. Manual journal entries can be easily used by management and employees to manipulate the numbers on the financial statements. As a result, much emphasis has been placed on journal entry testing. Such entries could possibly be entered in a company's accounting system on any day of the year by its employee, which makes it difficult and tedious to identify any potential fraudulent activities through manual means. Data analytics can be used in such areas to defend against fraud and management override by performing a more extensive search for unusual ledger activity to identify red flags.

Risk and fraud detection

Risk management can be supported by analytics in several ways. For instance, analytics may help to predict which customers are most creditworthy. It may also help in bad debt recovery. Even though bad debt recovery is typically based on the delinquency status of customer account, with a better understanding of customer circumstances and appropriate intervention, it may improve recovery rates and reduce cost.

In addition, analytics may help in fraud risk assessment by shaping the performance of specific audit procedures to address fraud risks. There is a shift from manual-based towards analytics-based fraud investigation. Traditionally, corporate fraud detection tends to rely heavily on the manual skills of the fraud investigation team using experience, instinct, and persistence to analyse data related to the fraudulent activity. Nevertheless, the sheer volume, velocity and variety of data that are now being generated every day in a corporation are likely to overwhelm fraud investigators' best attempts at data analysis. Therefore fraud detection has to evolve to be more technology-centric so as to make better sense of data.

Even so, it appears that most companies have not utilised analytics to provide better fraud detection insights to management and board. According to EY's 2014 Global Forensic Data Analytics Survey, only 7 per cent of the survey respondents are aware of any specific big data technologies and only 2 per cent are leveraging data processing capabilities in their Forensic Data Analytics programmes. Besides the challenge of 'digesting' big data, there seems to be inadequate awareness and expertise in fraud analytics within businesses.

A major reason that contributes to inadequate awareness of fraud monitoring and detection is the fact that there could be a false sense of security among businesses towards their risk exposure to fraud. This is possible as companies may not evaluate their internal controls regularly, hence overlooking or underestimating the sophistication of new fraud schemes and concealment methods, which often circumvent existing internal controls. In addition, being unfamiliar with fraud analytical tools that are available in the market could also mean businesses may not know what they are missing. Therefore it is important for businesses to know more about fraud analytics, and be familiar with fraud analytical tools that are available in the market. This will significantly improve overall effectiveness of fraud monitoring and detection in businesses.

Besides structured data, the availability of unstructured data sources such as text can also provide a wealth of analytical insights, from evaluating free-text descriptions for suspicious payment activities in accounts payable or cash disbursement journals, such as "respect payment," "friend fee," "help fee" or "problem resolution" to electronic mail communications indicating risk areas where fraud intent may be present. For example, banks can analyse a customer's current accounts, mortgages and wealth management (structured data) and spending habits/lifestyle of the same customer on blogs/discussion forums (unstructured data) to assess the customer's credit worthiness and the likelihood of him or her committing fraud. This may also improve existing credit-rating methods. By analysing both structured and unstructured data, companies are able to identify concealed patterns in financial, non-financial and textual data that would not otherwise be detectable with structured data alone.

Another example would be businesses may analyse unstructured data to investigate collusion. Unstructured data may reveal mismatches between the language people use when they are communicating confidentially to colleagues and when they are processing external transactions. The analysis of unstructured data is much more nuanced in the interpretation of language than is possible in the case of structured data.

A major challenge though, is the availability of fraud data analytics expertise. The reason is traditional audit and IT skills may not incorporate the more advanced data mining skill sets required for performing fraud analytics techniques. As such, it will be useful to have someone in the fraud investigation team who has big data and other advanced forensic technology skill sets to assist with gathering, validating and analysing the data and turning it into meaningful information. Ideally, this person should be someone who possesses database management and data analysis skills, in addition to anti-fraud and accounting-related skills. Furthermore, it will be useful to instil a fraud risk analytics culture within the business and develop processes for gathering, managing and reporting data in an efficient manner, as this will go a long way in establishing an effective fraud monitoring and detection programme.

In addition, the support by accounting programmes in universities is crucial to leverage our efforts to produce more analytics talents. Accounting programmes in tertiary education recognise the importance of data analytics and some have enriched their accounting curriculums by exposing accounting students to topics such as visual, text and fraud analytics. To strongly promote analytics courses to accounting students, we need support from the accounting and auditing communities. To recognise the significance of technology, professional certification programmes may wish to introduce more analytics materials, and include them as part of certification completion criteria.

Finally, greater effort must be made by the accounting profession to highlight the importance of analytics in accounting-related jobs. For example, with the emergence and rapid expansion of forensic accounting and business analytics, there is a great need for data mining skills, as well as forensic IT investigative skills. Consequently, the market needs to clearly signal the need for these skills in any job advertisement and position description.

The role of analytics in establishing an intelligent accounting function

Traditionally, the role of accounting function is viewed as that of a steward, rather than the catalyst for enterprise transformation and growth. 'Back office' is often used to describe the operating nature of accounting function. So in today's complex and uncertain business environment, the main challenge for accounting function is how to contribute and even lead the enterprise growth strategies while ensuring effective risk management and stewardship of the enterprise. The aim is for accounting function to create the insights that help make better corporate decision making, while continuing to ensure effective control of the enterprise. To do so, traditional accounting departments may have to rely on data analytics to transform themselves into 'intelligent accounting functions'. Intelligent accounting functions run their operations as cost effectively as possible, leveraging analytics to reduce accounting function's operating costs; strengthening stewardship and control so as to establish a solid foundation to support growth.

Analytics may play an important role in offering forecasting in an intelligent accounting function. For example, traditional annual business plans and periodic forecasts may not be enough in the context of intelligent accounting. Organisations need reliable, relevant and perhaps even real-time forecasting that is aligned with the changing needs of the businesses — robust scenario planning and sensitivity analyses. With reliable forecasting, companies can understand future scenarios, apply insights, and develop suitable strategies for response. By sharpening their focus on analysing data, forecasting trends and supporting business decisions that improve performance, accounting functions may become more intelligent, forward-looking and value-adding partners to business.

References and further readings

Gomes, L. (2011) Data analysis is creating new business opportunities, MIT Technology Review, 2nd May.

Miklos, V. and Chan, D.Y. (2011) Innovation and practice of continuous auditing, International Journal of Accounting Information Systems. (Special Issue on Research Methods) 12, 152-160.

CHAPTER 2

BUSINESS ANALYTICS AND BIG DATA PROJECT PLANNING

James Tan and Lee Yew Haur, SIM University

Introduction

With the advent of information and communication technology, it is becoming increasingly possible to leverage on the vast amount of digital information available today for making good decisions. For example, one can tap into the online reviews of hotels to decide where to stay for an upcoming vacation. For businesses, operational efficiency can be improved by using intelligent systems in the decision making process. For example, a computer can recommend whether a new loan application should be approved based on the credit history and profiles of the applicant. At the strategic level, the knowledge derived from customer feedback may prompt the management of a company to improve the service performance of its call centre, in order to improve customer satisfaction.

Big Data is a term coined to describe the scenario in which a diverse range of data in various formats is currently being produced and captured globally, and the vast amount of data is being generated at very high speed. A typical source of big data is the sales transaction systems, which log almost any kind of business transactions, such as cash withdrawals from banks, phone calls, ticket purchases, or itemising groceries at checkout counters. Another source of data is the social media platform, where numerous online comments, tweets, opinions, reviews and blogs are being captured by the second. Yet another source that contributes to big data is the scenario in which unique

smart devices are attached to entities, and these devices generate data and communicate with one another over a network. Such a scenario is commonly known as the Internet of Things. A simple example of such devices would be temperature and salinity sensors deployed in sea waterways. Such devices usually generate streams of data continuously, and when a large number of sensors are deployed, the amount of data generated will be huge.

Apart from the speed and volumes of data being generated, the format of big data can be diverse and complex. Traditionally, the scope of data analysis has been fairly confined to numerical and categorical data recorded in tabular format. But with big data, the format may include online reviews in textual format, images in graphical or video format, voice and music in audio format, and machine-readable format based on activity data captured by sensors and measuring instrument.

To unlock the knowledge or insight within Big Data, there is a need to apply analytics on the data, using techniques from disciplines such as data mining, statistical, and quantitative methods. Organisations will then have an edge over their competitors if they are capable of extracting crucial information that their business rivals do not know.

While many organisations have started to realise the importance of business analytics and big data, they do not know how to go about planning and executing their analytics projects. What are the critical aspects that should be considered when planning business analytics and big data initiatives? This is the question that this chapter attempts to answer. In short, there are three key aspects – business, data, and analytics, which we will discuss in detail.

The Aspect-Oriented Business Analytics Framework

There are currently several business analytics project development methodologies being proposed already. The methodologies provide a framework to guide practitioners in planning and executing analytics projects. For example, the Cross Industry Standard Process for Data Mining (CRISP-DM) (Chapman et al., 2000) is a methodology that consists of a six stages, starting from the business understanding stage all the way to the final stage, model deployment.

One key characteristic of existing analytics methodologies is that the planning and execution of the project involves largely sequential process stages. We argue that this may not be the most desirable thinking process for planning and executing analytics projects.

Indeed, we believe that the development of most Business Analytics and Big Data projects generally involves iterative refinements and alignments of three key aspects – Business, Data, and Analytics, as depicted in Figure 1. We have named this framework as the Aspect-Oriented Business Analytics Framework (AOBAF). This is a planning framework that could aid business analytics practitioners to consider the three aspects in order to improve outcomes of analytics projects.

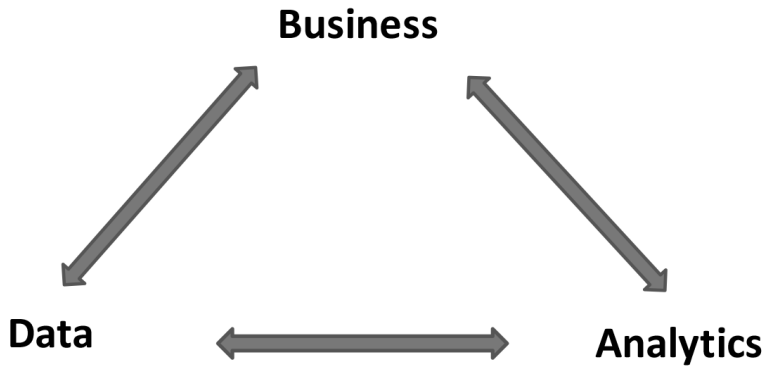


Figure 1: Aspect-Oriented Business Analytics Framework

In AOBAF, the *Business* aspect focuses on the need to define the business problem correctly and clearly. The *Data* aspect deals with the availability of data required to solve the business problem. The *Analytics* aspect deals with the application of analytics techniques on the given data, in order to address the business problem. While making sure that the three aspects are stated clearly, AOBAF also focuses on the pair-wise alignment of the three aspects as shown by the double-headed arrows in Figure 1. These alignments are critical as each of the three aspects cannot be considered in isolation. In the next few sections, we will discuss each of the aspects in details. And at the end of this chapter, we will use three case examples to illustrate how the issues shall be considered in each of the aspects as well as how the aspects should be aligned.

Business aspect

A very important starting point of a business analytics project is to understand the business aspect, i.e. defining the business problem and deriving the business objective. Without a clear understanding of the problem at hand, it is very difficult to craft an effective solution to address the business problem. Because this stage is concerned with understanding the business problem, we need not, and should not be concerned with the solution or implementation details at this stage.

However, sometimes we do find business user who are unable to articulate their business problem. Sometimes the wrong business problem may be identified. When this happens, we will need the domain expert to define the business problem clearly so that the project starts off on the right footing.

Once the business problem is clearly understood and defined, the scope should be refined so that the problem is specific and precise enough for the development of a set of possible solutions. Keeping an open mind will help one to find a comprehensive range of possible solutions.

It is important to note that not all business problems can or should be tackled using the analytics approach. For example, some business problems can be better solved by retraining staff with new skills, or by rolling out a new policy to strengthen checks and balances in a procurement process, or by introducing new measures to improve work safety in a petrochemical plant. Hence the possible solutions should include both analytics and non-analytics solutions.

Once a list of possible solutions is produced, objective evaluations have to be conducted in order to shortlist the top few solutions. If an analytics solution is identified as the most promising solution, we need to check whether the problem is really solvable using the analytics approach, and ask whether there have been successful applications of analytics to address a similar problem. Once the analytics solution is decided to be the best approach, the data and analytics aspects are then considered.

Analytics aspect

Once the business problem is clearly defined, the analytics aspect is then considered. Here, the key question involves asking what kind of technique(s) should be used for constructing the analytics solution. For example, if the business problem is to reduce customer attrition, then the analytics solution could be to build a predictive model to identify customers who are likely to churn, so that customer retention programmes could be introduced to keep these customers.

Sometimes the kind of analysis demands a particular technique that may not be available at the moment, or the technique may be in its early stage of research and development. In this case, the technique may not be mature enough to be used for any serious applications.

Another issue is whether we have sufficient information to apply a particular technique. Many analytics algorithms require the user to set parameters before it can process the data. For example, certain clustering algorithm may require the user to specify the number of data groups to be generated. This is often a tricky task because the user, in most cases, does not know the actual number of clusters present in the dataset. In this case, the analytics practitioner may need to generate a few clustering models (where each model is generated using a unique set of parameter settings) and evaluations would be required to find the most plausible model.

Data aspect

Once the business problem and the analytics solution approach have been clearly defined, the data aspect will consider the kind of data needed to address the business problem. In our previous example on building a predictive model to target and retain customers who are likely to churn, we would need customer records with fields that have pattern(s) related to the churn outcome. If such data is available, we could then use it to build a predictive model.

Apart from making sure that relevant data is available, we also need to ensure that the data is of good quality. This is because poor data quality (e.g., erroneous records) could result in an invalid model that distorts the true pattern actually present in the data. Hence, data with poor quality will have to be treated to ensure that reasonably good results could be obtained from the analytics process.

Sometimes the analyst may encounter a situation where the business user cannot define the business problem clearly. So even if the data is available, it is unclear how the data can be used to address the vaguely defined 'business problem'. There are two possible approaches to address this problem. The first approach is to revisit the business problem definition, and to make sure that the business problem is properly defined. The second approach is to explore the data first, so as to see whether there are patterns that are of interest to the business users. If the latter approach is taken, the project ends up being exploratory in nature. One very typical example of this is text mining of free-format customer feedback. This type of project is mainly exploratory in nature. The main goal is to identify key categories that are mentioned in large collections of textual records.

Pair-wise alignment of the three aspects

Once the three aspects are defined, the analyst needs to ensure that the pair-wise aspects are properly aligned.

The alignment between the business and data aspects involves asking whether the data is relevant and sufficient to address the business problem. Usually, the proposed analytics method assumes that the data contains certain pattern(s). If the data extracted is devoid of such pattern(s), we should obtain more data from the same source or other sources and combine it with the limited data that we currently have. Alignment of business and data requirements ensures that the data is sufficient in terms of relevance.

The alignment between the data and analytics aspects involves making sure that the data is in a form that can be understood by the chosen analytics algorithm. For example, some algorithms require data to be prepared in a prescribed format in order to ease or speed up processing. In this case, a set of data may have to be reformatted before it can be used by the chosen analytics technique. One typical example of this scenario is the conversion of unstructured textual data into tabular format so that it can be used by some data mining algorithms. On the other hand, the analytics practitioner may choose to modify the algorithm to read the new data format directly so that additional data pre-processing is no longer required.

Finally, the analytics and business aspects need to be aligned in two ways. Firstly, in light of the business objective, we need to consider the analytics techniques that are available to produce the kind of pattern that we expect from the data. For example, if the business objective is to use appropriate marketing campaigns to target different groups of customers, a solution would be to use clustering algorithm to segment a pool of customers into fairly distinct groups of customers. By doing so, a more targeted campaign can be applied to each group. Secondly, the patterns generated by the analytics technique have to be interpreted in the light of business objective. For example, a predictive model may generate a numerical score for each customer, quantifying each customer's propensity to buy a product. In this case, it makes sense to target only the top few percent of the most prospective customers so that the company is able to make the most profit from a marketing campaign.

In the following section, we will provide three case examples to illustrate how the AOBAF is used in real-world analytics projects.

Case examples

This section presents three real examples of projects using the AOBAF framework.

Case 1: Analysis of call centre problems using data visualisation

A key challenge for most call centres is to answer incoming calls from customers within a specified service target, say answering 80 per cent of the calls within 20 seconds. As the call centre is the first touch point for customers, any inability to connect them would have a negative impact on customer satisfaction. Therefore, it is imperative to determine the cause of the problem.

Business objective

- To understand why a call centre was unable to meet its KPI target for the service level and to take appropriate actions to improve the service level.

Data:

- Number of incoming calls aggregated by different time units;
- Service performance targets.

Analytics: Use plots to show the call volumes as well as service performance over daily time-slots in a typical week.

Alignment issue:

The alignment issue encountered is between the data and analytics aspects. The data mining practitioner had to experiment with different time resolutions when trying to identify service performance problem of the call centre. Time resolutions such as hourly timeslots over a typical day, and daily timeslots over a typical week were used. By using the daily timeslots, a heat-map plot reveals the day of the week in which the centre has the lowest service performance. Business domain knowledge is then used to validate the issue found.

Result:

The heat map in Figure 2 shows that Mondays have the highest call volumes and the lowest service level. Further investigation shows that more staff has to be deployed on this day because the call centre is closed on Sundays, resulting in more incoming calls on Mondays due to calls accumulated from Sundays.

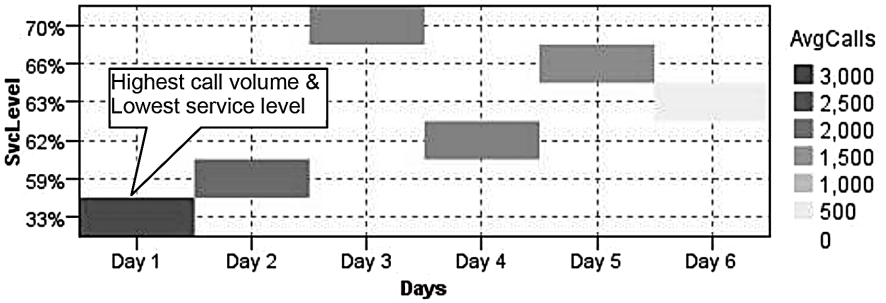


Figure 2: Day 1 of the week has the highest call volumes and the lowest service level.

Case 2: Text mining of call centre logs

Business objective: To identify actionable insights for process improvements based on descriptions found in the Call Centre Logs.

Data: Free-format textual description found in the call centre logs.

Analytics: Text mining of the free-format description to create distinct categories.

Alignment issue:
The alignment issue encountered is between the business and analytics aspects. Considering that the business objective is to identify actionable insights from the call centre logs in free-format text, the analytics technique chosen is text mining, and an appropriate dictionary of keywords has to be used so that relevant topics and concepts can be accurately extracted from the textual records.

Results: One of the main categories deals with frequent enquiries on the opening hours of the material collection centre operated by the university. As a result, the university has reviewed and improved on all correspondence and websites providing information on the opening hours of the material collection centre.

Case 3: Analysing customer purchase in a retail chain

Business objective: To better understand customers' profiles and purchasing behaviour so that appropriate marketing decisions can be made to improve customer satisfaction and grow the business.

Data: Sales transaction data that reflects when customers make purchases, how much they spend, etc.

Analytics: The sales transaction data over a carefully chosen period is summarised in terms of how recent, how frequent, and how much each of the customers made purchases.

Alignment issue:
The alignment issue encountered is between the data and business aspects. An appropriate time period for the study has to be carefully chosen so that it makes sense to make inference. For example, the time period cannot be too short so that it makes sense to infer that a customer might have churned because he or she has not made a purchase recent enough.

Results:
The method helps to identify a group of customers who used to buy a lot but are no longer making any purchases in recent months. These customers may be in the process of switching or have switched to another brand. There is an urgent need to introduce retention programme to bring these customers back.

Reference and further reading

Chapman, J. Clinton, R. Kerber, T. Khabaza, T. Reinartz, C. Shearer, And R. Wirth, CRISP-DM 1.0, Step by Step data mining guide. USA, SPSS Inc.,35-45, 2000.

CHAPTER 3

FINANCIAL ANALYTICS

Judy Ng and Ananya Sen, DBS Bank

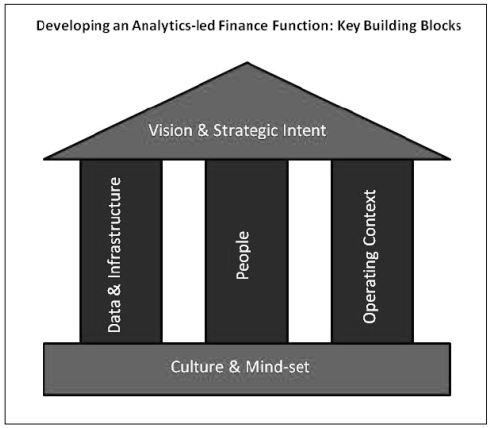
Introduction

The Banking context is changing driven by rapid pace of digitisation, explosion of smart-phones, and emergence of non-Bank players. Banks need to recognise that people need Banking, and don't necessarily need Banks anymore. Only those Banks who recognise this emerging reality, and who disrupt their own business model to stay continually relevant for customers, will survive and thrive.

This dynamic and evolving landscape is the new reality for the Finance function. To stay relevant, to add value, and to be truly seen as a business partner, the Finance function needs to fundamentally transform as well. Looking back and simply explaining historical performance will not be enough. Developing budgets based on static and largely historical trends will become of limited relevance. Providing simply a detailed cost summary and drivers of variance will not cut it either. Instead, Finance needs to truly embed and lead in analytics to elevate and shape the conversation in the organisation – to focus on what matters; to predict what is coming; and partner with key Business Leaders to ensure the organisation is pulling in the right direction.

In subsequent sections of this chapter, we highlight the key elements of this analytics led transformation journey for Finance, along with few simplified illustrative examples of how Finance can use analytics to partner business to identify potential areas of value creation, whether they be profitability of specific customer segments, underpenetrated customer groups, optimising the Balance Sheet, or managing Risk-Returns.

Developing an analytics-led finance function – Key building blocks



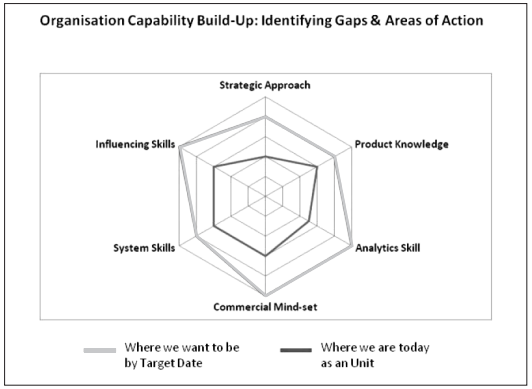
At DBS Bank, the transformation of the Finance function commenced in 2009 – 2010s as part of the overall strategic direction and aspiration set out by the Group CFO to revamp and fundamentally strengthen the Finance Organisation. We recognised early the value of operating as a strategic partner to the Business and Business CEOs and that it would involve re-configuring the way the Finance teams were organised. A key change was the creation of Business Finance CFO Teams closely aligned with each of our principal business groups – Institutional Banking Group, Consumer & Wealth Management Group, and Treasury & Markets Group.

The diagram above brings together the key building blocks of the transformation journey. These are mostly self-explanatory and well known to most organisations looking to make similar transformation. The critical point here is these building blocks must be tightly inter-linked and aligned to each other at all times to deliver optimal results.

Vision and strategic intent: From our own experience, creating a vision for Finance, where Analytics is central to what we do and how we add value to the Bank as well as deep commitment to that Vision, is the most important driving force for this change journey. It sets the mandate for both organisational change as well as requisite investments to make the change happen.

Data and infrastructure: Specifically, having a clear Vision and Strategic Intent helps to frame and get commitment to the scope of work and investments that are invariably required to build-out required infrastructure, end to end process and data management to enable analytics. For example, it commences from product capture to definition of data parameters and robust operational processes to ensure quality of data capture; integrated data warehouse including all product, customer, segment and financial details; creating the capacity to deliver daily balance sheets; or, risk-adjusted returns at customer group levels for institutional clients. Having the right infrastructure and data foundation is an absolute pre-requisite to being able to do value-added analytics at-speed. By that we mean if standardised data definitions are not in place, and there is no data warehouse and no data marts for example, it would be incredibly difficult to drive analytics within the organisation. The foundations must be in place or has to be built if not already there.

People: Having the right balance of people with the right mix of skill-set is a real challenge but also a big opportunity to differentiate and add value.



A good place to start is to develop a clear view of what are the skills and capabilities that are important and where are the key gaps. The right hand diagram sets out a simplified output chart of what such a gap-analysis might look like at an Unit level.

The illustrated dimensions are what we believe to be critical elements of any successful analytics-led finance function. In particular, a commercial mind-set and a strategic approach are two of the hardest elements to develop in finance people who might not have had a lot of business exposure previously. The gap analysis and findings are used in two important ways. Firstly, to develop tailored training programs – for example, within DBS Finance, we have initiated strategic problem solving skills as an important learning module to broaden perspectives and skills. Secondly, to identify areas where we will need to bring in new-talent to address specific gaps.

Operating context: Finance people generally are some of the hardest working people in the organisation, working long hours and carrying out many important roles and responsibilities. Often, however, the long working hours is driven by manual processes and workings.

Building up a team of analytically-minded, strategic and commercially-oriented finance people, and then asking them to carry out mind-numbing manual work-around, will be a huge waste of time and talent. Finance leaders would need to actively drive automation within finance and cut down on various Business-As-Usual historical pieces of work that simply isn't as relevant as before. For example, most if not all standardised reporting should be automated, with rich visuals and self-service capability for end-users who can then tailor standard reports to their own unique needs. These automation and simplification initiatives are most effective when driven by respective teams with deep knowledge of the processes involved. Depending on the scale of the initiative, it could also be set up as a formal project with broad-based project team members from Finance, Business, IT and others as required. A significant project that we completed recently involved building the capability to bring together data from various systems to get to customer level granular data and management information. The subsequent data then flows to pre-set up dashboards with rich visualisation for users of the report. In the past, getting to this level of granularity would have required significant manual work which would need to get repeated every month-end. The big point here is that Organisation Context, as we see it, is to create the right operating environment for analytically-minded finance teams to thrive in.

Culture and mind-set: For the finance organisation to successfully change, it is important that the culture and mind-set within finance evolves to a more strategic, commercial, analytics-oriented and proactive approach. Depending on the organisation, this can be a multi-year journey and organisations are using a number of different types of interventions to accelerate such change. Getting the linkages between the above mentioned building blocks right and making progress across each of them is not easy and requires significant time and resource commitment from senior Business and Finance leadership.

Opportunity areas for leveraging analytics in finance

In a sense, this is the hardest part - deciding opportunity areas to focus on. This invariably means what to prioritise and focus on and what to stop doing. Our view is that the analytical capability and resources should be focused on the highest value issues that the organisation is facing in consultation with business leaders. This could range from Balance Sheet management, Customer Value management, Productivity and Risk-Returns management, to developing business facing strategies.

We have highlighted below specific and stylised examples of how finance analytics can drive business action and value by way of context. These examples relate to Customer-level analytics and to Balance Sheet and Risk-Returns management.

Customer Strategy:

Winning strategies are focused on customer needs and a differentiated customer value proposition is critical to attracting and retaining customers. Crafting the right value proposition requires a thorough understanding of segment level economics and drivers of value. Analytics can play a significant role in this regard.

Table 1: Segment Mapping: Avg Revenue & Cost (Illustrative Data)

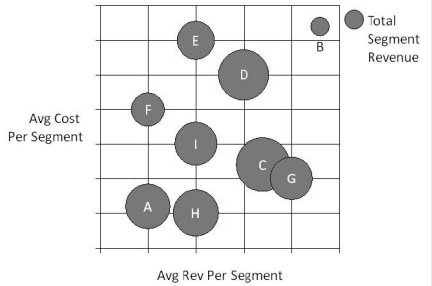
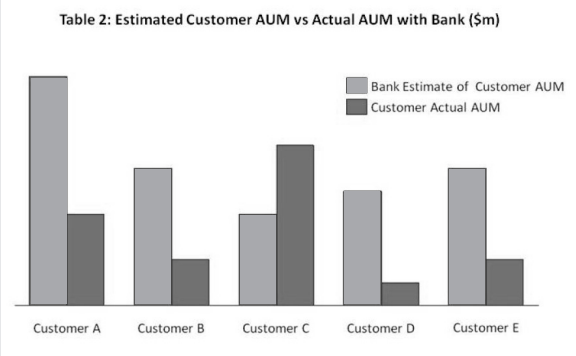


Table 1 shows an illustrative mapping of different segments, in terms of average revenue and average cost to serve customers in each segment. The bubble size depicts total segment revenue based on both interest income and fee income generated from customers in the segment. To get to the simplified chart and related insights is however not easy. It would require the data infrastructure and data capability to **a)** map each

customer to a specific customer segment based on pre-agreed segment criteria typically based on a combination of factors like demographics and customer behaviour and **b)** assess the total income generated from each customer across multiple products and often systems. For example, if a customer holds three products – mortgage, credit cards and a deposit account – in many organisations, these three products may be on three different systems and the customer level information needs to be brought together to give customer level income. Typically, cost-to serve data is more complex as it also requires taking into account a broad array of factors, like channel usage for example. The above analytic then forms the basis for more nuanced discussions of drivers of value for each segment and opportunity for action. For example, it could lead to specific cross-sell programs to fulfil unmet customer needs and drive segment value, as well as optimising cost-to-serve.

A second variant of customer segmentation-led value discussion is to analytically map our customer wallet share and opportunity headroom. This is especially relevant for the affluent segments which are often managed by a Relationship Manager and team of advisors.

Table 2 shows Bank estimates of customers' total Assets Under Management (AUM) based on customer conversation at the time of account opening and/ or subsequent conversations versus the customers' actual AUM with the Bank. In this illustrative example, looking at Customer D, we can see that the Bank has a fairly small share of total estimated AUM of the customer; whereas in the case of Customer C, clearly the Bank under-estimated the customers' AUM and would need to re-evaluate. This kind of "segment of one"

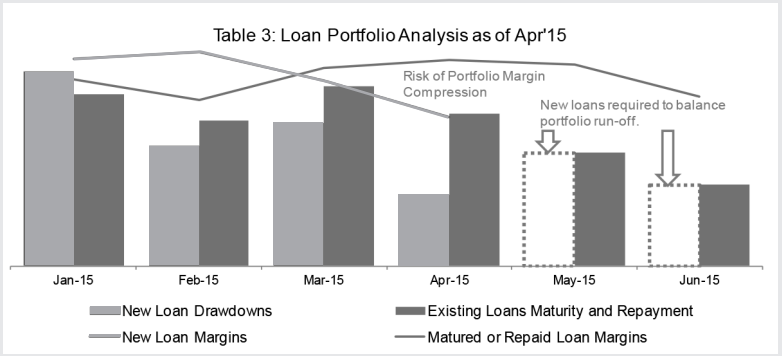


analysis at a customer level is especially relevant for the affluent segment. Relationship Managers can follow up with tailored discussion around customer need and investment opportunity based on client current asset allocation and mix with the Bank, as well as client risk profile and product suitability.

Balance sheet & risk-returns management:

One of the key challenges of Business Finance is to understand the construct of the bank's balance sheet. This broadly includes customer deposits and customer loans' portfolio mix of product types, maturity and behavioural profiles, as well as customer pricing and funding cost. Coupled with product knowledge, appreciation of external commercial and macro environment, Finance is a valued partner to businesses in identifying, monitoring and anticipating potential risks and seizing opportunities with regards to liquidity and product margins.

An application of analytics is where we utilise the repayment and maturity of existing customer loans profile. Overlaying this with approved loan pipelines and their expected drawdown dates/amounts, we could project the forward-looking loan positions as well as the ensuing margin. We look at the pricing level of new loan drawdowns and track transactions lost to competition as well as how our pricing levels compare with that of other



banks. To manage the balance sheet, we need a holistic view of the sources of funding, including customer deposits, their behavioural maturity profile as well as the cost of the different types of deposits. Table 3 is a pictorial illustration of how we look at a loan portfolio and we use it to engage in forward-looking conversation with businesses.

Another stylised example shown in Table 4 illustrates the distribution of the Risk-Adjusted Returns Performance of a segment of customers. Finance uses the information in engaging conversations with the Business Head to understand their account planning for the portfolio. The first category (<12%) is made up of customers whose revenue/net profit contributions fell below expectation against the Risk Weighted Assets (equivalent to capital) required to support the level of credit facilities granted. The second category (>12% to 15%) comprises those customers whose risk-adjusted returns are in the mid-range while third category (>15%) are those customers with clear superior returns. Consequently, the first and second zone customers present opportunities for the Business Head to evaluate how to improve the Risk-Adjusted returns or whether resources would be better diverted to other customer groups with superior returns.

Table 4: Return on Equity for Segment X by Entity Group*

Return on Equity	<12%	>12% to 15%	>15%	Total
Revenue S$'000	13,000	28,000	27,000	68,000
% of Total Revenue	19%	41%	40%	100%
Average Risk Weighted Assets (RWA) S$'000	1,510,000	1,414,000	814,000	3,738,000
% of Total Average RWA	40%	38%	22%	100%
Number of Customer Groups	10	15	9	34
% of Total Customer Groups	29%	44%	26%	100%

**figures are for illustrative purpose only*

The systematic approach to the use of analytics in approaching conversations with business on risk returns allow Finance to play a 'challenger role', which can lead to a more efficient deployment of the bank's scarce capital resources.

Conclusion

To stay relevant, to add value, and to be truly seen as a business partner, the Finance function needs to fundamentally transform and lead in analytics. This would require major end to end changes – from having the right infrastructure to people, culture and mind-set. Finance leaders need to take personal ownership in driving this change. The prize for getting this right will be huge for the Organisation as a whole. We wish you the very best in your own journey.

CHAPTER 4

INTERNAL AUDIT ANALYTICS

Tan Shong Ye, PricewaterhouseCoopers

Introduction

Leading organisations are able to gain significant competitive edge through data. The increasing sophistication of analytics technologies, coupled with the access and linkage of traditionally disconnected data sources, is providing a level of insight and perspective not seen before in large organisations. These same methods are rapidly making their way into Internal Audit, allowing auditors to better understand and quantify risk, test controls and business processes quickly and efficiently. Advanced analytics can uplift and even change the audit proposition.

In order to maintain their role of “Change Agents” and continue to be accelerators of organisational transformation, internal auditors need to be a trend-setter in technology usage. For many years, internal audit has focused on using data in limited ways to conduct analytics for fieldwork purposes — commonly known as computer-assisted audit techniques. With advancements in technology, ease of use and affordability of tools, now more than ever internal audit can focus on building a keen sense of direction to leverage data in a way that provides greater business insights, increases efficiency, enhances monitoring activities, and allows the company to respond better to risks. Leveraging data is not a destination of its own but, rather, a mindset shift to integrate data into the audit life cycle — from risk assessment to planning, fieldwork, execution, monitoring and reporting.

Data analytics in transforming the internal audit function

Internal Audit functions that leverage a more quantitative, data-driven approach to identifying and assessing risk, testing controls and reporting issues are more relevant to the business and can provide management and the Board more risk coverage with greater efficiency. Figure 1 enumerates some of the advantages of the use of data analytics for Internal Auditors.

Figure 1: Advantages of the use of data analytics for internal auditors

- Increased audit coverage through analysis of entire data population
- Reduction of time and cost of audit fieldwork through more focused planning
- Increased reliability of audit results and improved audit quality
- Early identification of trends in tested population
- Automated audit tests (Benford's law, duplicate payments, etc.)
- Simplified detection of fraud indicators, errors and abnormal operations
- Preservation of data integrity
- Ability to analyse transactions as they occur, instead of with several months delay
- Real-time identification of issues allowing rapid notification to management and immediate remediation

PwC's 2015 State of the Internal Audit Profession Study confirmed that the majority of Chief Audit Executives (CAEs) understand the value of analytics in improving coverage, depth and quantification of issues, and more timely identification of current and emerging risks. PwC's survey and interviews revealed that most, if not all, internal audit functions are thinking about how they can better leverage data to be not only more efficient but also far more effective. Most are experimenting with expanding its use particularly in such areas as fraud management, compliance monitoring, and risk analytics (Figure 2). While 82 per cent of CAEs report they leverage data analytics in some specific audits, just 48 per cent use analytics for scoping decisions, and only 41 per cent leverage on data analysis in their risk analytics. Thus many still report they have a substantial journey ahead.

Figure 2: User of data analytics in the internal audit function

Building data analytics capability

What can Internal Audit leaders do today to increase the maturity of data analytics in the profession (Figure 3), build its capability and capture the widespread and known benefits data analytics has to offer?

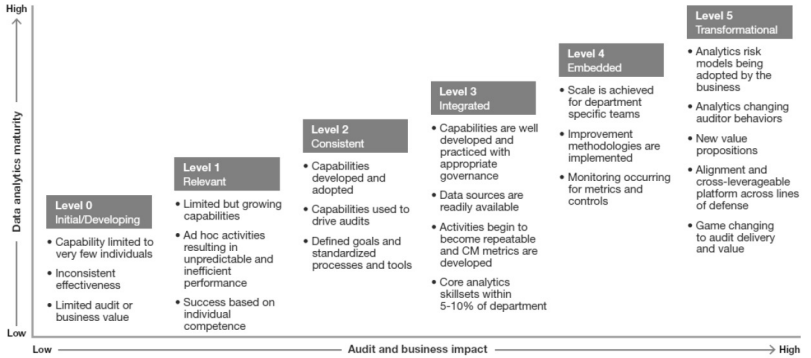


Figure 3: Analytics maturity model

Audit needs to overcome the traditional barriers to data analytics implementation. Research indicates that these barriers include: building and/or acquiring the right data analytics skill set; embedding data analytics across the internal audit life-cycle; identifying and acquiring appropriate technology; and gaining access to accurate, complete and relevant data in a timely manner.

Building the skill set: The skill set requirement for effective application of data analytics is quite different than that of the traditional auditor. For example, many traditional auditors are very comfortable with a judgmental assessment of risk and sample-based approach to selecting transactions for testing. However, the skill set needed to apply analytics holistically requires an analytical, quantitative and creative mindset. Without the right skills, Internal Audit struggles to synthesise various data points, understand the trends it identifies, and decide where to focus. This usually results in a reactive approach based on historical events compared to a proactive approach based on risk and trends. Many functions try to place equal responsibility on everyone to be a data user. In reality, most internal audit functions need a core group of "power" users with strong technical and analytical skills. These individuals serve the rest of the users in the department who are, in turn, trained to understand how to recognise the uses of data and synthesise the output.

Internal Audit must determine where they will acquire data analytics expertise. While some Internal Audit departments may have the resources in house that can be trained to provide the needed skills, others will need to acquire these skills in a scarce talent market. Rather than building an analytics team from the ground up, many organisations are recognising the value of leveraging outside experts. These firms are often better able to compete for the best talent, specialise in delivering the needed technical skills and offer the advantage of having already traveled the data analytics journey.

Fully embedding data analytics: As a first step into data analytics, many Internal Audit departments are focused on attempting to incorporate analytics into discrete audits, mainly in testing. They have not evolved to looking at data analytics across the internal audit life cycle. Furthermore, many companies start by directing analytics toward financial processes such as accounts payable or time and expense reporting as they are relatively "low hanging fruits." This narrow focus limits Internal Audit's ability to incorporate data into the identification and assessment of areas of higher enterprise risk. To increase the value of data analytics, Internal Audit should determine how to use analytics strategically around core risk and compliance issues. It should also leverage data in every aspect of the internal audit process, from risk assessment to reporting to on-going monitoring. By doing so, Internal Audit can add more impactful insights on a continuous basis and demonstrate efficiencies in how the function allocates resources.

Utilising technology: Internal Audit departments have not historically planned and invested appropriately for the technology required to routinely analyse data, whether that be simple analytic tools or more complex, enterprise-wide options (i.e., the spectrum of ACL/IDEA, Data Visualisation tools, and GRC tools). Technology should be viewed as an enabler and Internal Audit's short-term and long-term analytics goals will have a direct effect on the technology needed and the amount of training the Internal Audit department requires. This type of planning is essential to moving forward on embedding data analytics in the department's methodology and should be considered and built into the annual budgeting process. Although the shift in auditing approach and auditor behaviour will be a defining step in measuring your return on investment (ROI), the complexity of the technology should align with your department's longer term goals.

Gathering relevant data: Internal Audit departments continue to face challenges in obtaining timely, complete, accurate and relevant data. There are consistent themes related to data availability including: "multiple systems," "known data quality issues," "limited technology to download requested data," that Internal Audit must overcome once the previous hurdles of skill set, technology and embedding data throughout the audit lifecycle have been addressed. One step that can be taken to move past this barrier is for Internal Audit to evaluate what data other departments are using that could serve their purpose as well.

Partnering with other stakeholders, including IT, can be critical in determining what data sets are easily accessible and reliable. In addition, Internal Audit should narrow their data request, as much as possible, based on the key risk they are trying to address. Avoid the common desire to "get all the data" in order to determine where the issues might be as this often slows down the process or leads to frustration when the data request cannot be fulfilled. Rather, focus on the key pieces of data that are needed, where that data may already reside and who might already be using it. This will ease the data acquisition challenges. For example, if a concern exists pertaining to increasing DSO (Days Sales Outstanding), focus only on the data to analyse the calculation (such as invoice creation date and the date invoice is sent to the client). More granular data, such as invoice support details, may be available but is not necessarily key to DSO.

Strategies and processes in implementing a successful internal audit data analytics programme

Internal audit departments that successfully build data analytics capability recognise the importance of having a data strategy and the value of executing against that strategy. Further, the methods used by these audit groups are paving the way for bringing new ideas to business management in monitoring risk and control effectiveness, as well as introducing new forms of preventative and detective controls.

In these leading organisations, more than double the percentage of internal audit stakeholders see data analytics as highly valuable, indicating that strong data analytics drives strong overall stakeholder satisfaction. The journey to Internal Audit's integration of data analytics consists of assessing where the organisation is today in its journey, laying out a plan to build data analytics into the full internal audit lifecycle, and sustaining the data analytics capability over time.

Assessing where the organisation is today: To take significant steps forward, Internal Audit must evaluate what barriers have not been overcome in their data journey and ensure the data analytics plan addresses these barriers in a way that is aligned with the organisation's vision, and short- and long-term milestones. This includes agreeing on the people, skills, processes, technology and budget needed to successfully execute the plan. Certainly there is a financial and human capital investment required to build and sustain data analytics within Internal Audit. Careful consideration about both the initial and long-term investment approach is needed. This includes considering how to leverage the investments already made by a service provider rather than taking on the full burden of the investment internally. If done right, the investment in technology enablement and data analytic skills, whether built or acquired from a service provider, will not add to the total cost of the internal audit function but rather will shift resources from traditional approaches to more progressive data driven approaches.

Building the plan: When building the data analytics plan, it is critical to set achievable goals and milestones that align with Internal Audit's budget and skill and acknowledge the investment requirement. An example of an achievable goal includes an evaluation of how data could begin to be used to inform the risk assessment process this year, then be leveraged in a specified number of audits over a six-month period. Alternatively, start with how it could help with a specific area such as fraud risk assessment procedures. The key is to identify a logical starting point with reliable data that could build the foundation for how Internal Audit would adjust its audit approach based on the results of data analytics.

Effective planning requires a deep understanding of what data exists within the organisation, including where it is stored and how it is used by various departments. For example, during the formation of the audit plan for the year, Internal Audit could consider conducting an assessment of data sources that relate to known risks, link the data sources to the audit plan, determine which data sources could be obtained on a regular basis, and compare that to known data quality issues within databases outside of Internal Audit's control. As part of this process, Internal Audit should gain a better understanding of key performance indicators (KPIs) already being measured and what fluctuations in those KPIs mean to the business. By partnering with other groups such as Operations or Finance, Internal Audit can gain an understanding of how data is being utilised by these various groups, build on their work, and improve coordination. Such collaboration will help Internal Audit create an integrated view of risk across the organisation, perform continuous risk identification and assessment, and adapt its Internal Audit plan to narrow gaps in coverage. Finally, as part of planning, it is important to determine how the audit methodology will change to fully leverage the use of data analytics.

To assess if Internal Audit data analytic plan is robust and programme is on track, there are some key questions that should be answered to reach the data analytics goal (Figure 4).

Figure 4: Checklist of critical success factors

Organisation	• Do we build centralised capability? • What level of project management is needed? • Is the sponsorship message strong enough?
Human resources	• What skill sets do we have today? • What new skills are required? • What training is required? • Do we have a build or buy strategy?
Working practices	• How does this change our methodology? • Is data analytics embedded into every phase of Internal Audit? • How does this impact our strategy?
Technology	• What is already available to us and what do we need? • Should we build or buy new solutions and do any solutions already exist within the company?
Communication and reporting	• What is our role in reporting/trending remediation efforts of the business owners? • How are we educating audit practitioners on successful outcomes through the adoption of data analytics?
Knowledge management	• How will we share information with the other key business areas, such as Controller or Compliance functions?
Metrics	• How will we share information with the other key business areas, such as Controller or Compliance functions?

Data analysis tools and techniques

Internal auditors can use data analytics to provide a broad spectrum of services specifically designed to achieve audit objectives in a more reliable and cost-effective way. Internal auditors can use various data analytics software to mine data and do what-if analysis. Analytics technology, such as data mining tools and predictive analytics applications, are expensive and careful considerations are needed. The first thing to note is that the data analysis using SQL and SQL-like options (Microsoft Excel, Access, Oracle, Teradata) give you the basics of SQL query and analysis, but these are not alternatives to analytics workbenches or business intelligence suites such as ACL, Lavastorm, BusinessObjects, Cognos, MicroStrategy, Tableau Software, etc. The value of data analysis is often in finding correlations among disparate data sets or insights hidden in semi-structured or highly variable data sources that traditional SQL and SQL-like options may not be able to performed. For example, Internal auditors can use tailored analytic platforms (such as ACL, Lavastorm, etc) that have an extensive list of functionalities to perform data analysis of standard business processes, such as purchases and receiving of goods, payments, invoicing and invoice processing, master data management, pricing and IT.

Internal auditors should also leverage on the enhancements in data visualisation tools that made it easier and more intuitive for business users to access data and gain comfort with how data can be used. By providing a better view of risks, data visualisation tools are enabling internal auditors to absorb information in new and more constructive ways so they can identify and respond to emerging trends faster.

In conducting data analytics, Internal Auditors should develop methodology or approach (Figure 5) for the execution and define quality standards for analytics across audit planning and controls testing. A key to success in Internal Audit analytics is about understanding what data sources exist and how to efficiently leverage them.

Figure 5: Approach to data analytics

Assess and scope	• Define the objectives of the testing. What are we trying to prove/find out? • Hold planning meeting or workshops with the business to understand the processes underlying what we want to test. • Hold meetings with IT to understand how the related data is stored and how it can be extracted. Are reports available or will bespoke extracts need to be created? • Obtain sample data to verify understanding and avoid wasted time. • Define the baseline analytics required to determine the level of audit effort required? For example, in a shared service centre audit can Internal Audit evaluate the group's proposed KPIs and actual performance to see what specific processes might be higher risk and should be an area of focus during an audit?
Extract and transfer data	• Agree with the business/IT on what will be extracted, by when and by who. • Ensure that any scripts used are saved for future use with accompanying documentation. • Consider setting up extraction routines to be run out of hours to limit impact on business. • Agree on method of data transfer. Consider use of internal web based file transfer system or shared servers.

Validate data	• Check the accuracy of data. Consider comparing control totals on number of records or subtotals of value fields to other data sources, e.g. financial statements, MI reports. • Summarise key fields to generate overview of content of the data to highlight potential issues or limitations of analysis, e.g. does the data span the expected date range? does it include all expected information?
Analyse results	• Question the results. For example, what historical trends do the data show that provide insight into business risks (i.e.,business unit or specific location's profit margin quarter over quarter)? • Make sure you understand the business process supporting the transactions. Consider additional insights you can provide from the results of the analysis.
Reporting	• Define how the results of the data analytics conducted be communicated. Could your findings be communicated through a few succinct points using graphs or charts?
Monitoring	• Consider the repeatability of the data analytics review. How will your audit approach change if this area or process would need to be audited again? • What one or two analytics would help determine if a problem still exists or might be emerging?

The mindset within Internal Audit must fundamentally shift from a perspective of "Could we use data?" to one of "Our objectives are better addressed by using data. Viewed through the right lens, the data could substantially improve our understanding of this issue." In this new mindset, the team's thinking is focused on which analytics may be applied and how that might replace or supplement previous audit approaches.

Reporting of internal metrics that illustrate how Internal Audit is embracing data analytics will help build and sustain momentum for change. Addressing these key areas will be vital to long-term sustainability.

Summary

PwC's 2015 State of the Internal Audit Profession Study clearly indicated that stakeholders expect more from Internal Audit. A data-focused approach allows Internal Audit functions to identify issues, target risks and allocate resources more effectively. Whether Internal Audit departments build the skills internally or partners with a third party provider to overcome the barriers to success, those that can adjust in more real-time and establish an end to end data driven Internal Audit model, will elevate their relevancy and allow them to move from simply auditing around historic risks to monitoring and pivoting based upon prospective risks. Ultimately, the result of incorporating data analytics is companies can be confident that Internal Audit is allocating resources against the most important objectives and the greatest areas of risk, therefore obtaining maximum value from the audit work scoped and performed. Listed below are three case studies that demonstrate the benefits of using data analytics by internal audit teams.

Case study 1

The internal audit team of one's of the world's largest retailers faced a challenge to identify, detect and analyse potential fraud indicators within their sales function. The internal audit team developed a list of potential fraud indicators ("red flags"), designed data tests, extracted sales data and performed data analysis. Based on results obtained within a reduced timeframe, the internal audit team was able to capture major sales trends, increase the reliability of audit results, expand scope of the audit, obtain meaningful insights on potential fraudulent activities and select specific transactions for substantive testing.

Case study 2

The internal audit team of a regional airline used data analytic tool and tailored them in accordance with audit objectives, which in turn enabled the internal auditors' team to shorten audit fieldwork, decrease the volume of manual testing, enhance the reliability of audit results and increase the scope of their audits. The internal auditors' team was also able to use the most advanced and matured features of the data analysis tools to perform Continuous Auditing ('CA'). CA has completely changed the internal audit paradigm from retrospective, sample-based and cyclical control activity to an automated, real-time review, covering 100 percent of transactions. CA was combined with Continuous Control Monitoring ('CCM'), which is put in place by management to ensure that policies, procedures, and business processes are operating as expected.

Case study 3

A U.S.-based public utility is early in its journey of continuous auditing and data analytics. This 10-person Internal Audit group began by targeting areas of data analytics focus, interviewing stakeholders, and building support from management. It was particularly important to gain IT support to both understand data issues and to gain access to the desired data. The team focused on building and leveraging relationships in IT, and brought data analytics depth, discipline and technical talent to the project. Inevitably, one view of data would lead to the desire to look at it another way, so having the data, tools and skills needed to re-aggregate the data in various ways, and drill down on short notice, was important to early success.

Ultimately the project resulted in visibility and specific actionable data on individual employees, functions, locations and business units that helped gain CEO's and CFO's attention and strong support. The results have been used with the COO and other business leaders to generate discussion and action on areas not previously visible to the company.

In reflecting on Internal Audit's performance, the CEO, CFO and audit committee chair all identified this as an area of significant internal audit value. The utility's Internal Audit team now is working to sustain the momentum, incorporating data analytics as a key aspect of its strategic plan.

CHAPTER 5

RISK AND COMPLIANCE ANALYTICS

Tim Phillipps and Sean Dunphy, Deloitte Singapore

As previous chapters have established, analytical techniques and approaches are increasingly applied to a wide range of strategic and operational areas. While analytics may have been the domain of select teams, buried deep within the business, it is now firmly on the C-suite agenda. As we know, risk cuts across organisational boundaries — internal boundaries within an enterprise as well as customers, suppliers, alliances and partnerships that form the wider business ecosystem. Analytics draws on data across these increasingly open, interconnected networks to provide actionable insights. Put simply, risk analytics is a critical capability in developing and sustaining a competitive edge at a time when risk issues affect business strategy more than ever.

For virtually anyone working in the area of risk management, analytics isn't new — risk professionals have been using analytics tools for years. But many have noted a resurgence of interest in the application of analytics to risk management challenges, and with good reasons. First, sophisticated tools and techniques from statistics, computer science, and operations research are more readily applicable to data from a wider range of internal systems, let alone to "Big Data." Second, whether it's at home or in the work place, we have to come to expect the latest available data to inform a choice. Lastly, new means of creating value have been developing in the form of interactive and fluid configurations of economic relationships and activity — so-called "business ecosystems" and platforms — and smart businesses around the world are responding, widening the perimeter of risk. The proliferation and democratisation of data, together with the extension of analytical techniques and technologies, arrives just as the issue of risk takes on an even higher profile.

Risk leaders face mounting pressure to identify a wider range of risks, and better understand the impacts of differing economic environments and potential events. They are expected to facilitate the holistic management of broader, finer grained risks, and to back these assessments up with hard data. That can be a tall order for organisations relying on the same old approaches to risk management. As the steward of strategy execution in an ever-accelerating competitive environment, a rigorous, data-driven approach finds a very natural home in the risk management function.

Some key applications of analytics to risk

Analytics is the practice of using data to manage information and performance – and make smarter decisions at the point of impact. It can apply to every function of the enterprise but most organisations tend to focus on five main areas of decision-making and operations: customer, supply chain, finance, workforce, and risk. In each of these areas, analytics can help direct strategy and operational improvements. To do that, it integrates capabilities in data management, statistics and other quantitative methods, change management, technology, automation, and governance into a powerful agent for making better and faster decisions.

One reason analytics is on everyone's radar is that it is easier than ever before to extend analytics capabilities throughout the organisation, pushing deep into the heart of the business: "proofs of concept" have been demonstrated and widely documented across functions and industries; data and analytical technologies are more readily available; new generations are more digitally savvy. Intuitive dashboards with automated workflows and role-based views now empower front line staff, while business analysts have self-service tools to manipulate data from a variety of sources. No longer is analytics the exclusive preserve of "data scientists" or management team off-sites; it's about enabling the decision-making process at every level of the enterprise.

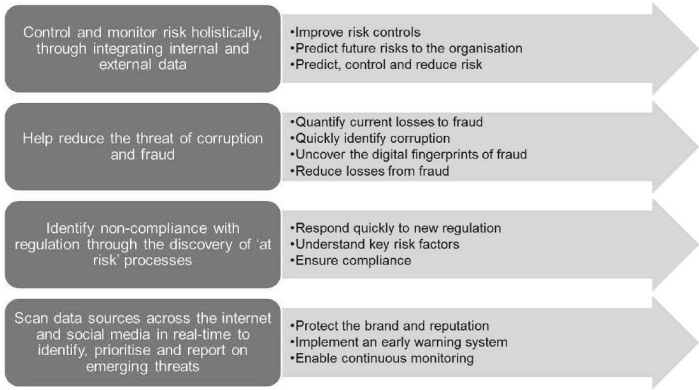


Figure 1: Benefits of risk analytics

Within the risk function, these developments are driving two major changes. We see risk taking advantage of new analytical methods — descriptive, predictive, and prescriptive analytics — and bringing those capabilities to the core to improve the efficiency and accuracy of these functions or add a new lens. We also see risk bringing its cross-functional perspective and capabilities to the challenges and opportunities faced by other parts of the business, such as pricing, or vendor spend analysis or technology investment prioritisation.

For instance, risk touches virtually every aspect of talent management, and talent touches virtually every aspect of risk management. But few companies systematically encourage their talent managers and their risk managers to work with each other in collaborative pursuit of the organisation's broader goals. Consider talent management professionals' typical view of their job. Their stated responsibility is to find, keep, and motivate the talent the company needs to run the business — not, on the face of it, to manage risk. Yet that is just what they must do if they are to manage talent effectively. In a sense, talent management's entire core mission is to reduce the risk of not having the right talent to as near zero as possible. In addition, there's the perennial need to address the spectrum of risks inherent in any employer-employee relationship: poor performance, fraud, and employee health and safety, just

to name a few. All of these issues need to be considered to manage talent effectively, and not even the most conscientious talent managers can do it alone.

Risk managers, for their part, come to their job from a completely different angle. Their stated responsibility is to help align risk exposures with strategy — not, on the face of it, to ensure that the organisation has right talent to run the business on an enterprise-wide scale. Yet that is just what they need to do if they are to manage risk effectively. For one thing, certain risk management responsibilities need highly skilled, specialised professionals to carry them out — professionals who seem to be getting harder to find and to keep. Furthermore, a great deal of organisation risk has its roots in factors related to people: how they think, what they do, the principles they hold, the norms they follow. All of these issues need to be considered to manage risk effectively, and not even the most capable risk managers can do it alone.

Analyse this

A growing number of companies are embracing workforce analytics as a powerful talent management tool. Workforce analytics applies advanced statistical techniques to workforce and demographic data to help uncover and alert leaders to possible talent challenges (such as a high likelihood of voluntary turnover) with respect to both key individuals and the workforce in general. As such, this technique can be an invaluable aid to both workforce planning and talent management.

Beyond its role in talent management, however, workforce analytics can offer insights into employee-related risk in any area, provided that risk correlates at least somewhat with employees' demographic, personal, and workplace information. The same statistical tools that can tell leaders that employees with longer commutes are the most likely to leave the company, for example, can also reveal which employee populations tend to be more susceptible to risk events such as absenteeism, accidents, or fraud. Leaders can then use this information to focus their resources on programmes and workforce populations where their efforts can have the greatest impact on these events; in fact, the emerging discipline of safety analytics concerns itself specifically with applying workforce analytics to employee health and safety issues.

We have seen few companies that have even begun to tap the potential of using workforce analytics to identify leading indicators of employee-related risk. Until the practice becomes widespread, using work force analytics can be one of an organisation's most distinctive sources of competitive advantage.

In this sidebar illustration as for other domains, it is up to boards and the senior management to encourage the integrated view that analytics enables. One way to begin is to establish an ongoing dialogue between risk and, in this case, talent to consider analytical insights: Sit them down with each other to discuss the ways in which talent and risk affect each other; have them identify potential concerns that warrant a closer look; ask them what should be done about each; and connect them with other groups in the organisation — functional and business-unit stakeholders — that must contribute to any solution.

Clearly, effective risk management can't just be top-down — or sideways, as the case may be. This is precisely where analytics comes in play, effectively connecting top-down and the bottom-up approaches. The role of the risk function is rapidly evolving, with integration at the core of its mission. Enabled with data-driven insight, risk can not only provide the connective tissue but also be the driving force for intersecting initiatives even as the C-suite expands to include roles such as chief analytics officer, chief digital officer, and chief data officer.

The Risk Intelligent Enterprise

Beyond specific areas of application, by pulling together many strands of risk into a unified system and providing additional clarity in identifying, viewing, understanding and managing risk, analytics helps to establish a fact-based baseline for measuring risk across the organisation. Taking a unified approach to risk management is a key component of becoming a Risk Intelligent Enterprise™ — one in which boards and executives integrate risk considerations into strategic decision making, and where business units and functions incorporate risk intelligence into many of the actions they take. The Risk Intelligent Enterprise (Figure 2) outlines three essential components of effective risk management. Each of these components is necessarily underpinned by a foundation of analytical expertise, processes and technology:

- Risk governance, including strategic decision-making and risk oversight, led by senior management and the board of directors
- Risk infrastructure and management, including designing, implementing and maintaining an effective risk program, led by executive management
- Risk ownership, including identifying, measuring, monitoring, and reporting specific risks, led by the business units and functions — customer, finance, supply chain and talent, among others

The top level, risk governance, directs the Risk Intelligent Enterprise. It defines the parameters of acceptable risk, monitors strategic alignment and sets overall risk management expectations. The bottom level of risk ownership, in turn, is what risk governance relies on to execute Risk Intelligence. This includes all of the functions' and business units' responsibilities with regard to identifying, evaluating, mitigating and responding to risks in accordance with risk governance mandates.

The middle level, risk infrastructure and management, forms the essential link between risk governance and risk ownership. Composed of the three "pillars" of people, process and technology, we believe that an effective "common" risk management infrastructure — that is, an infrastructure that supports consistent risk management approaches throughout the organisation — is essential to give executive management an enterprise-wide view of risk.

As we illustrated in the talent example, activities across all these levels are integrated into a systematic, enterprise-wide programme that embeds a strategic view of risk into all aspects of business management.

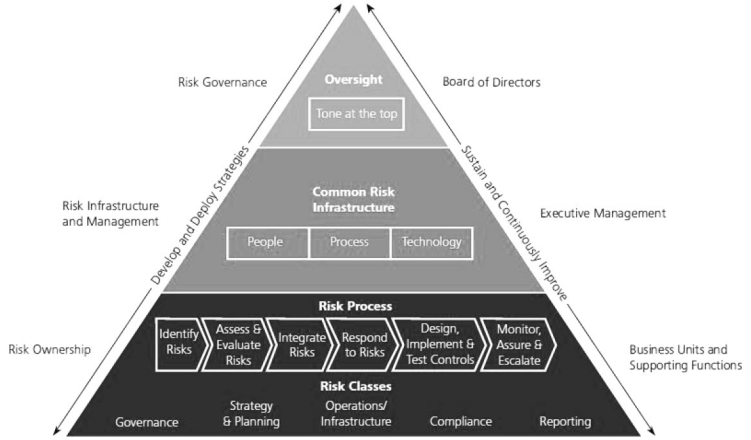


Figure 2: The Risk Intelligent Enterprise

In a Risk Intelligent Enterprise, business units (departments, agencies, etc.) are responsible for the performance of their business and the management of risks they may take within the risk framework established by executive management. Among other things, risk owners are responsible for identifying, measuring, monitoring, controlling and reporting on risks; promoting risk awareness; and reprioritising activities as dictated by data-driven, risk analyses. Risk owners do not determine the organisation's risk appetite — they stay within the tolerances determined by executive management, based on consistent definitions of risk classes, data sources, analytical methods, and conventions for reporting. In this context, the governance-related risks associated with insufficient succession planning can be better understood; strategies and plans can consider the potential impact of changing demographics on future workforce requirements; risk factors can be assigned to divisions, sites, processes, shifts and even to specific employees.

Compliance analytics

Compliance is an enterprise-wide risk, yet traditionally it may be the risk that has commanded the least attention from corporate leadership. Other types of risk — strategic, operational, financial — receive a great deal of attention as they are often regarded as risks that a company may choose to take to advance its strategic plan. Compliance, in contrast, is often seen as a necessary evil, a risk without a corresponding reward.

Regulators now expect absolute traceability in control and compliance, from the front line to the boardroom, following the approach that "if you could know, you should know" and setting standards accordingly. The way in which regulators expect many companies to organise their compliance efforts also sets compliance apart from the other risk classes listed at the bottom of Figure 2.

Many companies are creating a centralised compliance function to consolidate oversight of compliance programmes. No equivalent function is likely to exist for the other risk classes. While the compliance function is a risk owner in its own right, it is also responsible for helping to maintain enterprise-wide consistency in how compliance risks are rated, controlled, documented and reported. Analytics can help to identify "at risk" processes and poorly defined controls, including improvements to data gathering and integration.

Although compliance is often seen entirely in terms of "keeping the business out of trouble," that's only half the story. The other half is the potential for a company's strengths in compliance risk management to help create new value. How? By opening the door to opportunities that companies with weaker compliance capabilities might consider too risky to pursue.

Let's imagine that a company is contemplating a business opportunity in a country where bribery is a common business practice. The revenue potential could be huge — but so is the inherent risk of violating anti-corruption regulations, such as the U.S. Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, or Singapore's Prevention of Corruption Act. If leaders lack confidence in the company's anti-corruption controls, processes and oversight procedures, they might forego the opportunity, reasoning that the increase in residual compliance risk would outweigh the potential revenue gains. In a company with strong anti-corruption programmes and controls, however, leaders might well embrace the opportunity, judging the company's corruption-related risk management practices up to the job of keeping the related residual risk within their tolerance level.

The scale and pace of regulatory change demands a new approach or, at the very least, a revisit of the information strategy. Better alignment of information management strategy across business functions and initiatives will provide an opportunity to rationalise and update technology, and overcome data silos. Opportunities include:

- Automated monitoring of regulatory releases, sometimes coupled with business process management tools to automatically alert responsible parties to relevant changes
- Workflow capabilities to facilitate compliance process execution and tracking and to promote individual accountability
- Integrated "front end" interfaces that allow users to execute, document, and track compliance activities in multiple areas from a single point of access
- Automated reporting and dashboard tools that can consolidate compliance information from sources across the enterprise, and succinctly display key compliance risk and performance indicators

Social media and digital risk

In an increasingly digital era, many organisations face a daunting challenge: how to compete in a socially powered world? Used effectively, social media can provide tremendous opportunity to engage with a large audience, build relationships and drive brand affinity.

When organisations are faced with the task of implementing a social business strategy they can often encounter several barriers, notably in appropriate risk management. Challenges can include:

- *Tracking social media:* Understanding your social presence is important not only from an operational perspective but also from legal and regulatory standpoint. An integrated view of social activity requires the implementation of the right processes and supporting technologies.
- *Managing multiple accounts:* As organisations expand their social media presence, it becomes increasingly complicated to manage multiple accounts used internally by employees, and externally by third-party agencies.
- *Keeping record:* Content on social media sites can be legitimately presented and used in a court of law. It is important that organisations build mechanisms to archive content and make it easily accessible when needed; this may even include user-generated content.
- *Multiple layers of approvals:* A number of organisations impose various internal approval stages before content can be shared on a social platform. These approvals may be perceived as barriers to achieving the desired outcomes, but the right process can not only reduce the cost of compliance, they can also augment the quality of engagement.
- *Consistent application of policies:* Applying a single set of rules to the diversity of social platforms may not be practical, and could lead to non-compliance.

The usual caveats about technology apply. A technology solution is only as effective as the process it enables; much of the benefit depends on managing change among users; and setting realistic expectations is vital to the perception of value. However, if effectively implemented and used, today's compliance tools hold the potential to drive substantial improvements in both information quality and process efficiency.

Data as an asset

We know that every organisation — large, medium or small — depends on reliable data. Managed well, it will drive revenue, reduce costs and mitigate risk. Managed poorly, it can lose customers, inflate costs and expose business to unbound levels of risk. In this context, data can no longer be viewed as an inert by-product of doing business. Instead, organisations must recognise that data is an asset and a potential source of liability.

As organisations rely ever more heavily on the information produced by their systems, a comprehensive data management programme is critical. The quality of data in an organisation can be degraded due to multiple sets of the same information across divisions, poor data import, poor control over data acquisition and data transfers as well as poor security. This can potentially cause reputational damage and lead to poor decision-making due to incorrect information, wasted investment, errors in financial statements and compliance issues.

We've touched on the appointment of chief data officers as a catalyst to address these challenges and opportunities. Indeed, it's increasingly necessary for a dedicated data organisation with a top-down mandate to champion data management rigor and promote stewardship. An enterprise data roadmap provides a framework to understand, manage and execute cross functional initiatives to meet regulatory and strategic imperatives. Key benefits include an increased focus on insight based on a common, integrated view rather than manually intensive data collection and reconciliation of

fragmented, incomplete data. The organisation gains the flexibility to meet changing regulations and there is greater confidence in taking key business decisions regarding capital deployment, market and business investment.

A discussion of Risk Analytics & Compliance wouldn't be complete without giving some consideration to "Big Data." While "Big Data" can undoubtedly provide a new window on the world, the right analytics can clarify the view and help to understand what it means for the organisation.

Misuse of the term "Big Data" has rendered it meaningless or, at best, ambiguous. Here's a practical and useful definition: structured and unstructured data generated from diverse sources in real time, in volumes too large for traditional approaches and legacy technologies to capture, manage and process in a timely manner. It includes data from websites, blogs, news feeds, social media, and public and private databases. "Big Data" also includes data from the core business as well as the extended business of suppliers, other partners, and customers.

"Big Data" also has the potential to bring added risk and compliance challenges, as discussed in the text box on digital and social media, as well as increased privacy requirements, data retention obligations and exposures to cybercrime. Ultimately, the value of "Big Data" depends on an organisation's ability to analyse it in useful ways while simultaneously strengthening its data management capabilities. Hence, the scale and quality of analytical capabilities to harness "Big Data" are also areas that risk leaders could very reasonably include within their purview.

Case studies:

Safety analytics for a global mining company

A large mining company was seeing a flat trend in their injury rates, but an increase in their fatality rates, and did not know why. It was taking them a month to generate an injury incident report and they were not able to integrate different sets of data to see what could be a factor in injuries.

Data was integrated from various sources and presented through an interactive dashboard. In particular, the dashboard also integrated data from the following sources and analysed how they affected each other: demographic information, time entry, maintenance, human resources, production bonus, and safety reports. A new metric was introduced: injury propensity — the likelihood that an employee would be injured on any given day.

The organisation was able to review these different sources of information for the first time to draw some actionable insights:

- They noticed a high propensity for injury among student workers, and implemented more safety training.
- They also noticed that injuries spiked after people were promoted, possibly due to a lack of additional safety training when an employee transitioned into a new position.
- Safety Incidents were also more frequent towards the end of the month. The client noted that safety training happened in the first 10 days of the month.

Through closer dialogue between risk, human resources and production departments, and crucially, through integration of previously disparate data, this organisation was able to improve its operational and financial risks as well as its compliance.

Customer insights enabled by data quality

A leading financial institution faced a daunting challenge: How to reduce risk exposure and better serve and market to its customers. The institution lacked a consolidated view of its customers that would help satisfy regulators and meet lending authority requirements. When auditors reported a need to limit the bank's customer credit exposure across all product lines, the bank was ill-equipped to respond. With customer information housed in disparate source systems, the bank lacked access to the well-defined and accurate customer data necessary to meet legal and audit demands. Adding to its challenges, it had no framework for translating customer information into effective marketing and customer service.

The financial leader turned to Deloitte to develop a foundation for improved customer information management. The result was a reusable framework that can scale to meet the changing needs of the business. Deloitte's framework and approach consisted of data profiling and analysis, data cleansing and remediation, master data management (MDM) mapping and modelling, and designing data management and governance structures.

The project kicked off with a two-month data quality initiative. Since our client lacked data standards, Deloitte worked with the team to define standards to profile against and prioritised project components accordingly. By linking its critical data, the client was able to identify and join supplemental customer data to this common point of reference as well as line-of-business data, such as product-related data. Deloitte developed a data integration plan to help manage risk, which included a customisable data quality scorecard to assist with ongoing monitoring of data quality.

Deloitte's analysis and framework gave our client the customer insight needed to satisfy regulatory and audit requirements and better market its services to customers. Through this approach, the bank now has consistent, better defined customer data. Their new-found ability to aggregate total loans by customer has reduced risk exposure. With a holistic view of its customers and their relationships to their accounts and to one another, the client has improved its effectiveness in marketing and risk assessment.

Fraud analytics for a retail company

A retail organisation was experiencing fraudulent activity in some of their 100 branches and saw returns deteriorating. The company had knowledge of one type of fraud but recognised that they might not have the full picture. They wanted to see how analytics could help them see where fraud was potentially occurring, ways it could have been carried out, and areas they needed to monitor more closely.

The company found that their employees were able to manipulate stock-taking processes and procedures in their systems. This, combined with the ability to provide a discount or refund to the customer and earn commissions on sales, meant that employees had the opportunity to commit a combination of different types of fraud. These potential frauds were not detectable due to control weaknesses in internal systems. The challenge was to try and distinguish the different types of potential fraud and figure out how to analyse the data in order to show where fraud was taking place, how frequently, by whom, and the costs associated. The techniques and results needed to be robust so that innocent people were not labelled as fraudsters.

Combinations of analytical techniques were used to correlate certain types of behaviours displayed for what was understood to be a fraudulent activity. For example, certain types of products that are easily sold, returned and refunded were correlated. The types of products, as well as stock-take variances and stock-take adjustments taking place in branches were profiled. These tell-tale signs were used to detect potentially fraudulent activity. The next step was to look at who did what by integrating this information with audit logs to compare levels of refunds with the levels of stock write-offs, and the seniority of staff who processed these transactions. The "genetic code" of a fraudster and a description of what types of things to look for made it easy to see anomalies in the data, and pinpoint the area in which there were issues.

References and further readings

"The Three-Minute Guide to Risk Analytics," 2012, http://public.deloitte.com/media/ analytics/3-minute-guide-to-risk-analytics.html

"Corner Office Analytics: Chief Risk Officer," 2014, http://www2.deloitte.com/us/en/ pages/deloitte-analytics/articles/corner-office-analytics-cro.html

"Crunchy Questions for Sticky Issues," Deloitte, June 2011, http://public.deloitte.com/ media/crunchy-questions/pdfs/us_ba_crunchy questions_060911.pdf

"Business Systems Come of Age," 2015, http://www.deloitte.com/us/ businessecosystems

CHAPTER 6

FRAUD DETECTION AND DATA ANALYTICS

Lawrance Lai and Sidarth Khashu, EY in Singapore

With the increased use of technology, businesses have seen a staggering increase in volume, variety and velocity of data. This "big data" is being leveraged to strategise, innovate, compete and, in some cases, outperform their peers.

While technological advancements have provided new business opportunities, it has also increased avenues for fraudulent behaviour[1], not only in the traditional areas of purchases, payroll, sales and accounting, but also from faceless fraudsters working from any part of the world.

An effective mechanism to manage the risk of fraud in today's data-driven business environment is forensic data analysis (FDA). FDA provides insights that drive you to see what you would otherwise never expect to see. It helps organisations scan each data point within enormous data sets in an effective and efficient manner to generate meaningful information, which is easy to comprehend and valuable for decision-making. It uses both "structured" (transactional data like finance or operational data) and "unstructured" (free text communication like emails or social media messages) data sources for detecting and, in some cases, predicting fraud with a high degree of probability. This involves integrating statistics-based tools, unstructured data tools such as key word search, data visualisation and text-mining tools and traditional rule-based descriptive queries and analytics.

[1]For the purpose of this paper, we will limit our discussions of fraudulent behaviour or fraud to 'occupational fraud' or frauds committed by an individual or a group of individuals to the detriment of an organisation. See www.acfe.com *for more details in respect to occupational frauds.*

Different areas of fraud and their detection methods

There are few truly unique types of fraud schemes in the recent past; those that appear to be so mirror the changes in economic environment or advances in technology and prevalent business models. While there are various ways in which frauds are commonly categorised, the Association of Fraud Examiners (ACFE) in the US has identified three broad forms of occupational frauds that capture the most commonly seen fraud schemes. These are asset misappropriation, financial statement fraud and corruption.

Figure 1: Types of occupational fraud

	Asset misappropriation	Financial statement fraud	Corruption
Broad definition	Theft or embezzlement of assets of an organisation	Manipulation of financial records through understatement or overstatement of revenue, expenses, assets or liabilities	Abuse of trust or office for personal gains
Examples	Inventory theft Cash theft Fraudulent payments Unrecorded business transactions	Non-recording of expenses or recording operational expenses as assets to overstate assets and profit Booking fictitious transactions Improper valuations of assets	Bribery Provision of favours to parties in exchange of financial benefits
Impact per 2014 ACFE Report to the Nation on occupational fraud and abuse	Most common (85 per cent of cases reported) and least costly (median loss of US$130,000)	Least common (9 per cent of cases reported), however caused greatest financial impact (US$1m)	Middle of the road (37 per cent of cases reported and median loss of US$200,000)

According to 2014 ACFE Report to the Nation on occupational fraud and abuse, tip-offs or whistleblowing is the most common method for detecting occupational frauds. In 2014, whistleblowing accounted for more than twice the rate of any other detection methods, and nearly half of all such tip-offs were provided by employees.

While fraud detection continues to be challenging, organisations can do more in managing fraud risks through proactive anti-fraud mechanism and not leave things to chance.

Effective and comprehensive anti-fraud mechanisms require organisations to pursue and implement systems that support early identification, thorough investigation, followed by disciplinary actions for any suspected or reported fraudulent behaviour. While the proactive system acts as deterrence, a consistent and comprehensive response to fraudulent activity cautions perpetrators that fraud is taken seriously and that action will be taken.

For early fraud detection, organisations should adopt a two-fold strategy. First, there must be the right tone at the top that encourages transparency and rewards individuals who speak up against fraud. This is critical in defining how the organisation is viewed by internal and external stakeholders. Having an appropriate culture is also important as research suggests that fraud is often committed by insiders – people who understand the systems well, or even senior management personnel who abuse their position of power to override controls.

Second, they need to undertake periodic fraud risk assessment of their business operations in order to develop practical anti-fraud strategies to address the gaps identified. These strategies could range from implementing specific anti-fraud controls within a business process, to making long-term investments into innovative technologies that can assist in real-time detection of and predicting potential fraudulent behaviour.

Identification of anomalies and risk areas using data analytics

Traditionally, financial ratio analyses have been used to highlight red flags for financial statement manipulations. Today, technology is helping us move beyond the traditional rule-based queries to advanced analytics that drill deeper into financial and operational data to produce small sets of suspicious transactions.

Benford's law, a relatively simple and well-used computerised technique, is often used to identify potential anomalies in data sets. Benford's law defines logical patterns of the digital sequence in naturally applied numbers and can be used in multiple ways to analyse data for fraudulent behaviour. While Benford's law does not require expensive data analysis tools and is easy to learn and implement, it should be considered just as a routine check for occupational hygiene in data sets. Benford's law has limitations, such as an expected deviation percentile between expected and actual frequency, as well as the inability to work with random (e.g., lottery) and non-naturally occurring numbers (e.g., telephone numbers).

Advanced FDA does more than that. As shown in the EY FDA maturity model below, leading FDA practices incorporate elements of all four quadrants to ensure more effective detection and fewer false positives.

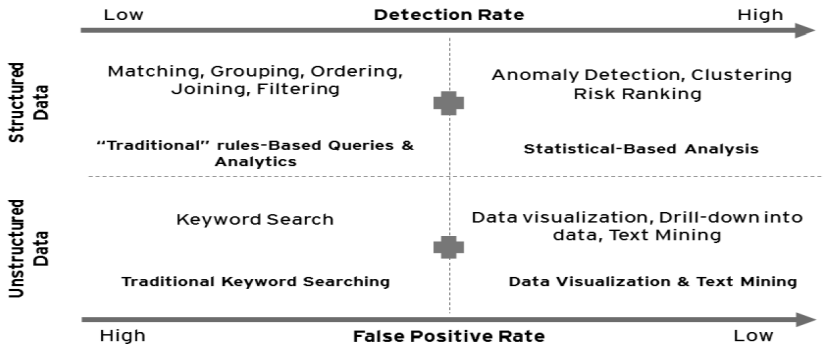


Figure 2: FDA maturity model

FDA analyses can be classified into the following broad categories:

Retrospective statistical analyses

Retrospective or look-back analyses are post-event analyses. When deployed over large data sets, such analyses can pinpoint anomalies derived from multidimensional attributes within the data. Some of the key enablers for such analyses include sector-specific maturity models, fraud scheme rule sets or libraries, and standard data models. An important aspect to be considered for such analyses is the appropriate cut-off time period. Various factors such as changes in business processes, operations, or IT systems will have a direct impact on the nature of available data for the period selected and the results.

Apart from financial statements, two operational areas where retrospective FDA is often used are procurement and sales. Analysts use the data to identify out-of-pattern analyses, outlying transactions and linkage analyses to develop rules to spot unusual trends and specific transactions.

For example, a large corporation conducted a retrospective FDA of its Procure to Pay data from multiple locations over two financial years, which revealed unusual patterns of costs and payments. This included payments of specific vendors being processed prior to agreed payment terms, minor differences between budgets and price quoted by the winning bidder, and unusual hikes in prices shortly after the bidding process. When the data analyses were followed by background searches and investigation, it was noted that an employee's relatives were awarded contracts (at sites different from where the individual worked) and confidential budget data were shared with them.

In another example, forensic analyses of distribution and customer data at a pharmaceutical company issuing drugs as samples to medical practitioners revealed misappropriation of these samples as well as bribery and corruption by some medical practitioners.

In addition to structured data, unstructured data is also now being used to address concerns of fraud and vulnerability through different data analytics techniques. These include:

Fraud Triangle Analytics (FTA) – Also known as sentiment analyses, FTA analyses the language used in emails and chats against a library of key words associated with the Fraud Triangle factors[2]. This determines whether expressed statements or opinions in a document are positive, negative or neutral. Organisations can use this data to identify potential fraud conversation and understand the sentiments or motivations behind an identified fraud.

Link or Social Network Analyses – This evaluates relationships or connections between organisations, people and transactions. Link analyses is used on applications like phone records and internet access logs, while social network analyses uses data available on social network sites like LinkedIn and Facebook to identify related parties, conflict of interest, and subtle patterns of behaviour. Along with background searches on individuals and entities, such analyses often uncover hidden relationships and unwarranted nexus.

[2]*Fraud triangle theory by criminologist Donald Cressey suggests that three factors (incentive, opportunity and rationalisation) need to be present in an environment for fraud to occur.*

Concept Clustering – Along with electronic data review, millions of transactions can be analysed for similar themes, patterns, words, and sizable groups can be created for each theme. For example, payment transactions or emails can be analysed for specific periods and words like "gifts", "under table" and "incentives". These can then be categorised accordingly and investigated in a time-bound manner.

Predictive or forward looking models

Predictive data analyses uses techniques like data mining, statistical modeling, machine learning and artificial intelligence to develop intelligent scorecards and powerful business rules, which enables prediction of potential fraudulent activity with a reasonable degree of probability. By applying predictive analytics, large corporations use patterns in historical and transactional data to identify future risks and opportunities. While such analyses are usually used to identify riskier areas of business, they can also be used to highlight suspicious cases on a real-time basis and live authorisation of compliance for sensitive and high-risk transactions.

It is important to note that work for predictive data analyses requires significant investments to understand the business operations and associated fraud risks. While having a statistical background is essential, analysts building the predictive models need to understand the business well enough to recognise if results of the mathematical models are meaningful and relevant. Sometimes, it is also important to gather external data and conduct periodic review of the information used for updates, which could impact the predictive model.

For example, a global corporation was using many service centres around the world for payment processing. Given the value and frequency of payments across each centre, it was imperative to use advanced technology for fraud detection. As part of its development of a real-time fraud detection mechanism, vast amounts of data from different sources were correlated and analysed, and bespoke mathematical models and algorithms were created to highlight potential high-risk transactions from the payment processing software. Once implemented, each payment processed was automatically filtered through these rules and an additional level of approval was implemented for transactions highlighted as high-risk by the system.

In another example, a life science company used predictive data analyses to build a model indicating potential predictors of corruption. Once implemented, all requests for sales events were reviewed against such predictors for approvals. Six months into operationalising this model, the compliance team saw an automatic reduction in the number of events being organised at unusual locations, increase in the number of pre-approved vendors being used and could correlate rates charged by third parties across events and locations.

Advanced visualisation of analytics

Visual analytics or advanced visualisation of analytics is not a technique, but a tool that provides insights in an interactive graphical manner. Data visualisation has proved to be effective as humans are better equipped to absorb data in a visual form than displayed in numbers of texts.

As part of an FDA exercise, the scores from the analyses are fed into data visualisation software. Such software converts these scores into visual formats, including meaningful multi-dimensional charts and dashboards, which not only allow easy understanding of the analyses, but also enables one to see results from different criteria and analyses with a click of a mouse.

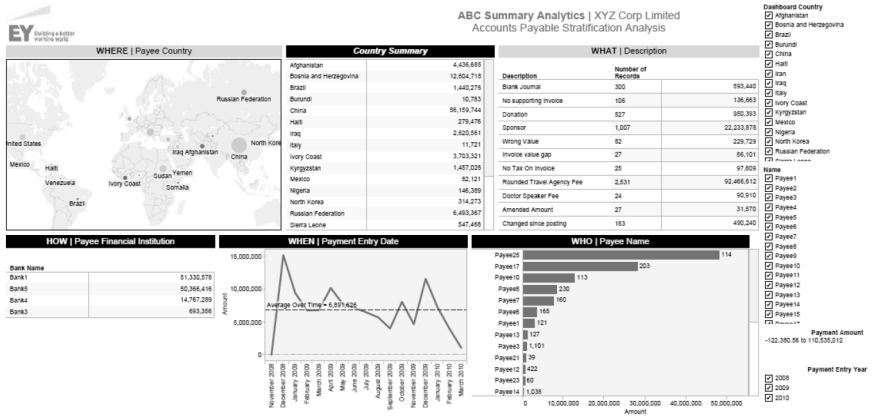


Figure 3: An interactive dashboard in Tableau

In Figure 3, account payable data analysed for an organisation is presented in an interactive dashboard, which is easy to comprehend and also provides users the ability to further analyse or investigate the data for other concerns.

The availability of computing power and the use of the internet have made the process of FDA easier. However, computers and technology alone cannot and do not carry out the analytics. Human manual intervention is essential to understand the raw data, create queries and provide the necessary interpretation. In the absence of people who do not have forensic, mathematical or statistical background, there could be a tendency to extrapolate too far and the findings can become meaningless.

How to detect fraud through data analytics

Before and during the process of fraud detection through FDA, it is important to consider these key factors:

Data requirement and collection

The first step is the identification and collection of data to be analysed, which is driven primarily by the objectives and areas under review. A key aspect to consider is the fraud test definitions used on the data. The fraud tests or indicators are based on experience, typical business operations and rule limits, and common fraud schemes.

For example, if the analyses are to be conducted on payroll data, some key fraud tests would include possibility of ghost employees, duplicate bank details, common bank details between employees and third parties, and payroll processed outside of the usual payment period. The forensic analyst and the person driving the exercise must hold multiple discussions with the custodians of the data to understand the business operations and data flow within the organisations.

One common pitfall is not spending enough time in understanding the data that is available and required for the analyses, as well as the data that is not available. Similarly, data source should not be limited to financial statements or management information systems. Data is available from a variety of sources, such as security records, CCTVs, recording devices, emails, downloads from online sources, and individual or corporate searches.

Another common mistake is the tendency to analyse all available data. Useless data takes time and effort to process and reduces efficiency. Also, maintaining additional useless data means additional cost for the organisation. Thus it pays to invest time to understand the IT systems and data flow at the organisations and the data set required for analyses. The request should also be discussed with the IT personnel to identify the best possible format in which data can be collected.

Data collection is critical both from a completeness and forensic perspective. While it is important that the analyst checks the completeness of data collected, it is also important to collect the data in a controlled environment, especially if the analyses are to be used or defended in a court of law.

Data cleansing

Once collected, data needs to be reviewed and organised prior to analysis. Often, data collected is incomplete, contains errors or duplicates, or is mapped incorrectly. Incorrect data will generate wrong results and mislead users.

Some of these errors also arise from the manner in which the data is extracted, and data validation prior to analysis is critical. Given the volume and complexity of data sources, this usually means automating the process, but it doesn't mean humans cannot be involved. While a few inspections and validations can be manually undertaken, there are specialised cleansing tools available in the market. Our experience has shown that investing efforts to understand the data substantially reduces the time spent on false positives, and potentially addresses IT design gaps.

Use of forensic analytics (or data processing)

While no single hardware or software satisfies all requirements, the selection of the tools and techniques must be based on factors like performance, functionality, usability and cost. Organisations should look at the leading practices and software available in the market to identify the one that fits their requirements. While, in some cases, in-house software may work depending on the kind of analyses to be conducted, organisations must be aware that there may be limitations depending on the nature of tests that can be undertaken.

Organisations should compare the cost of building an in-house software against buying a license of a tried-and-tested one. Once the software is identified, it is important to develop the various tests that would run for the purpose of the FDA exercise. Customising tests according to the nature of the business is crucial to achieving meaningful results. It is also important to note that data analytics is an iterative process. The initial findings must be reviewed to further clean the data and reduce possibilities of false positives.

Evaluation and reporting

Fact-based evidence gathered through data analyses can drive actionable decisions and help to focus investigative efforts where it matters. While evaluation of data is not purely data analytics, it requires close coordination between analysts and the user. It is important for the user to understand the analyses as much as the results.

Two common pitfalls observed at this stage are that users confuse facts with opinions and they tend to use the initial results to confirm pre-existing biases. Users should always consider limitations of the analyses, including possible angles that have not been considered before finalising the results. It is of paramount importance to note that not all outliers observed are fraud. Users need to objectively assess each outlier for negating other possibilities including false positives such as unusual but legitimate expenses that are duly approved, possible manual errors in data entry, and changes in business process not captured by the data. Analysts and the user should discuss the actions performed from the data gathered and determine additional steps that need to be performed.

When reporting the results of data analytics, it is important to demonstrate the usage of scientific methods and facts that can stand the test of court. The language or style should be adapted based on the audience and in a manner that is suitable for non-technical individuals. The reports should describe the actions performed and those that need to be performed. In cases where reports are submitted as evidence in a court of law, the analyst is also required to provide a written expert conclusion of the evidence provided.

Conclusion

FDA provides business executives the ability to comprehensively look through large data sets and spot unusual patterns or anomalies that are otherwise invisible. To build a dynamic and effective FDA program, leaders should:

- Start simple and focus on low-hanging fruits. Targeted analytics provide greater benefits to the organisation in terms of knowledge and value.
- Spend time to understand business operations and leverage existing knowledge of sector-specific fraud risks within your organisation. The success of FDA depends heavily on the accuracy of the business rules created for the risk framework.
- Take actionable results to management. Nobody likes results that are not measurable and actionable.
- Bear in mind that sustained FDA success within an organisation takes time and depends on the technology used, experience of the investigators and end users who can interpret the results.

Disclaimer
The views reflected in this article are the views of the authors and do not necessarily reflect the views of the global EY organisation or its member firms.

Part 2
Shaping your cybersecurity strategy

CHAPTER 7

CYBERSECURITY CONCEPTS AND STRATEGY

Calvin Chan, SIM University

Introduction

The emergence of Business Analytics served as a springboard for business innovation among many companies and government agencies. Business analytics involves the use of data mining and quantitative analysis techniques to derive insights from large amount of data (i.e. Big Data). These insights help managers in making better decisions and enable organisations to produce innovative products and solutions that correspond with market trends. Consequently, data has been declared to be the 'New Oil' of the 21st century, positioning it as a valuable resource. For example, supermarkets have huge amount of data on the consumption habits of their customers collected through their Point-Of-Sales systems. These data can be aggregated and analysed to provide insights to manage their product stocking more efficiently. These data can also be mined to identify customers for targeted upselling marketing campaigns.

As the value of data rises, the corresponding risk in ensuring the security of data also rises. Data security breaches can translate into severe financial and reputational damages. With data protection acts (e.g. Singapore's Personal Data Protection Act) in place, companies are also subjected to regulatory compliance to safeguard data in their custody. Cybersecurity can no longer remain as an afterthought but requires strategic attention as part of a company's governance and strategic IT planning.

Traditionally, companies have left cybersecurity to the onus of IT professionals and cybersecurity experts. However, such approaches to managing cybersecurity are no longer sufficient under contemporary regulatory regime and intensifying cybersecurity threat landscape. Business managers and executives need to play a larger and more direct role in managing cybersecurity. For this to happen, business managers and executives need to be better acquainted with cybersecurity concepts. Hence, this chapter can be seen as a move towards this end as it introduces a conceptual framework on cybersecurity strategy to business managers and executive in planning for and evaluating their firms' cybersecurity strategy.

Ensuring the C.I.A. of data and information

The goal of any cybersecurity strategy is often summed up as the triad of C.I.A., i.e. confidentiality, integrity and availability.

Confidentiality

Confidentiality ensures that only persons with the appropriate privileges and rights have access to the data and information. It is closely associated with the concept of privacy, which focuses on the rights of the data or information owners in determining and controlling how their data and information are to be accessed and used. In contrast, confidentiality concerns with ensuring authorised access to data and information and not about ensuring the rights of the data and information owners.

In recent years, cyber espionage has become a key threat to confidentiality of data and information. The prime targets for cyber espionages are governments and large enterprises. Cyber espionages are often hard to detect as they often do not cause disruption to the system or corruption to the data. Its main aim is to remain dormant and maintain surveillance for an extended period of time.

One cybersecurity threat that is often associated with cyber espionage is Advanced Persistent Threat (APT). APT is a form of stealthy and continuous (hence persistent) hacking process which often target specific individuals or organisations to gain access to the system. Once the system is penetrated, the perpetrators will maintain control of either pilfer data and information or attempt to broaden its access within the system. These may carry-on for an extended period of time in stealth. APT involves the use of advance hacking techniques and complex coordination. As such, APT attacks are often state-sponsored.

Since the launch of the Personal Data Protection Act in Singapore, there have been a number of high profile breaches of confidentiality reported in the media. In one case, a school mistakenly sent out an email with an attachment containing the personal data of 1,900 pupils to parents. In another case, the computer system of a karaoke chain was suspected to have been hacked and the personal data of 300,000 members was subsequently posted online. These two examples illustrate what is known as data leakage where confidential data and information is 'leaked' to unauthorised parties.

In addition to data leakage, there are also other manners that confidentiality can be compromised. For example, user IDs and passwords may be stolen by unauthorised personnel to assess a company's computer system. Confidentiality is also compromised when staffs share their user IDs and passwords with unauthorised personnel, or permit unauthorised personnel to access confidential data and information on the computer.

Some of the common measures used in ensuring confidentiality include data and information classification, data encryption, access authentication and rights management tools. Data and information classification is a discipline of classifying data and information into categories. An example of these categories can be Open (which may indicate for open access by everyone), Confidential (which may indicate for access by anyone in a firm and no need for encryption), and Secret (which may indicate for access by selected individuals in a firm and requires encryption). Access authentication and rights

management tool will be used to authenticate the credential of a user through the user ID and password. Upon successful authentication, the user will be granted access to the appropriate categories of data and information.

Integrity

The next item in the C.I.A. triad is integrity. Integrity is understood to be the state of being complete, whole and uncorrupted. Data and information integrity is about ensuring the authenticity of the data and information as being free from corruption, damage or destruction.

One of the most common challenges to data and information integrity is computer virus attacks. Computer virus can damage the integrity of data to varying degree, depending on the malicious design of the virus. At an innocuous level, it may just make superficial changes that are easily reversible. At a more malicious level, the data may be irreversibly corrupted or erased.

Breaches of confidentiality can also compromise data and information integrity. Kaspersky Lab, a Russian cybersecurity firm, announced in February 2015 that banks around the world have lost up to US$1 billion due to breaches of confidentiality and integrity. Hackers would gain unauthorised access to the banks' systems by 'spear-phishing' its employees. 'Spear-phishing' is a form of cyber-attack that targets specific organisations or individuals. Spoof emails are sent to these organisations or individuals to trick them into clicking certain malicious hyperlinks which enable the attackers to gain access to the systems. Once these attackers are in, they would compromise the integrity of the data by transferring money to accounts under their control.

Some measures that can be used to uphold data and information integrity include anti-virus software, cyber surveillance and monitoring system, keeping system logs and audit trails, using analytics to identify irregular activities. Unfortunately, most measures do not directly prevent data and information integrity comprises from occurring, but serves to mitigate the impact and enable corrective actions to be taken.

Availability

The final item in the C.I.A. triad is availability. Availability means enabling authorised access to data and information in a desired format on-demand, without interference or obstruction.

Interference or obstruction to data and information available is mainly achieved through network and system outages. A common approach to obstruct availability of data and information is through Denial of Service (DoS) attacks. In a DoS attack, an overwhelming quantity of requests is sent to the targeted computer server (e.g. a web server or network server) to an extent that the server is unable to cope with the request load such that it starts to slow down and subsequently fails. There is a variant and more sophisticated form of DoS attack known as Distributed Denial of Service (DDoS) attack. DDoS attacks typically involve the use of a large number of computers, known as bots, to overwhelm the targeted server. These bots may not even be owned by the attacker but the control of the bots was seized by the attackers through viruses. Hence, even if a company may not be the target of a DDoS attack, it can still be implicated if its computers are seized to become bots to launch an attack.

Although there is no foolproof approach to prevent a DoS or DDoS attack and ensure availability, anti-DDoS technologies are now available to mitigate such attacks. One approach employed in anti-DDoS technology is to redirect network traffic to traffic scrubbing filters. A key function of these scrubbing filters is in differentiating traffic sent by the bots and legitimate traffic. Only legitimate traffic will be directed to the targeted server. More advanced anti-DDoS technology may even incorporate behavioural analytic tools to identify malicious attack traffic. However, such analytic tools often require calibration by experienced and knowledgeable cybersecurity experts which are currently in short supply. To address this, some vendors are now providing managed anti-DDoS emergency response services to companies that cannot or do not want to set up an in-house anti-DDoS function.

Multi-Layered approach to cybersecurity

While understanding cybersecurity concepts such as the C.I.A. of data and information is important, business managers and executives will also need to be mindful in adopting a multi-layered approach to Cybersecurity. As it is not possible to categorically ensure confidentiality, integrity and availability of data and information, a multi-layered approach allows for a more comprehensive cybersecurity strategy as the layers serve as a tiered security structure. In the unfortunate yet highly plausible scenario of a cybersecurity threat penetrating through one of the cybersecurity layers, there are other layers in place to mitigate and counter the impact of damage.

There are altogether five layers in the multi-layered cybersecurity approach. These are prevention, protection, mitigation, respond and recovery. Description of each of these layers is provided below.

Prevention

Prevention focuses on measures that stop or avoid cybersecurity incidents, which jeopardise the confidentiality, integrity and availability of data and information, from occurring. Such measures can be technological or social oriented. Preventive technological measures include installing virus scanning software that scans through all incoming files to prevent against virus attacks. Essentially, preventive technological measures concern the use of technological tools to stop or avoid cybersecurity incidents.

On the other hand, preventive social measures are initiatives that target at people in order to stop or avoid cybersecurity incidents. For example, cybersecurity campaigns, seminars or newsletters can be leveraged to create greater awareness to cybersecurity threats among employees and avoid social engineering related threats. Social engineering, in the context of cybersecurity, refers to using behaviour manipulation techniques to manoeuvre individuals to perform certain actions that compromise cybersecurity. These tasks may involve the divulgence of authentication credentials such as user IDs and passwords, or visiting certain malevolent websites that contain virus. In fact, within the realm of cybersecurity, human has often been cited to remain as the weakest link. Hence, no cybersecurity strategy is complete without any preventive social measures.

Protection

Protection is about having measures to safeguard and secure the data and information. For instance, sensitive data and information can be protected by employing cryptography technology. Access control technology can also be used to protect against unauthorised access to sensitive data and information.

When considering protection, the needs for physical security to protect the data centre where sensitive data and information are housed have often been overlooked. This can be dangerous as physical damage to the servers and databases will also affect the data and information. Hence, it is important to not focus only on online but also the offline security measures needed in safeguarding the data and information when looking at protection.

Mitigation

Given the dynamicity of the cybersecurity threat landscape, it is impossible to totally prevent and protect against cybersecurity incident. In fact, given the current state of technology development, it is still not possible to prevent and protect against some cybersecurity threats such as a DDoS attack. The only way to counter a DDoS attack is actually considered to be a mitigating measure as the malicious traffic is redirected rather than being eliminated. Hence, there is a need to have in place mitigating measures. Mitigation focuses on limiting the impact and reducing damage in the event of a cybersecurity incident.

Depending on the type of cybersecurity threats, mitigation measures can take on many different forms. It can take the form of specific counter measures such as anti-DDoS technology as discussed above. It can also take the form of the architectural design of the information systems. For instance, a demilitarised zone (DMZ) is often found in most enterprise information architectural design. The DMZ is a sub-network within the enterprise information architecture where servers offering external facing services are located. Examples of such services include Internet webmail services or e-commerce services. The DMZ is segregated from the internal network where more sensitive data may be housed. In the event of a cybersecurity incident due to the external facing services, any damage caused will only be limited to the DMZ.

Mitigating measures can also be process-based such as having in place a Business Continuity Management (BCM) plan. For example, when an operationally critical system is not functional due to cybersecurity attacks, the BCM plan can kick in to ensure that the business can continue to operate and function.

Respond

Respond is about having responsive measures that directly address or counter cybersecurity incidents after the incident has occurred. It focuses on dealing with or eradicating the cybersecurity incident. For instance, when a computer virus is found on a company's computer, there are tools such as anti-virus software to detect and clean off the computer virus.

Considering the scale and complexity of the cybersecurity threat landscape, there is growing limitation to the type of respond measures that an individual company can adopt. Increasingly, some degree of national or even international coordination is required in responding to cybersecurity incidents. For example, when a company is under DDoS attack, the bots launching the attack are likely to be coming from around the world and international coordination is thus needed to put down the bots.

Recovery

The last layer is recovery. Recovery should happen in the aftermath of a cybersecurity incident, when the cybersecurity incident is eliminated or resolved. It focuses on restoring from the damage inflicted by the cybersecurity incident. Nevertheless, in some cases, it is not possible to completely restore back to a pristine stage, resulting in irreversible data or information lost. For instance, a computer virus may have wiped out some data or corrupted some files. If the damage is not reversible, an alternative will be to extract the data or files from the most recent backup. If there is considerable gap between the time that the backup was done and the time that the computer virus struck, any work since the last backup will be lost. Hence, recovery should not be an afterthought, but needs to be considered and planned ahead in order for it to be effective.

From cybersecurity concepts to strategy

While the C.I.A. of data and information and the Multi-Layered Approach to Cybersecurity may appear as independent concepts, the two can be combined into a conceptual framework on cybersecurity strategy (as shown in Figure 1) and used for both planning and evaluating cybersecurity strategy.

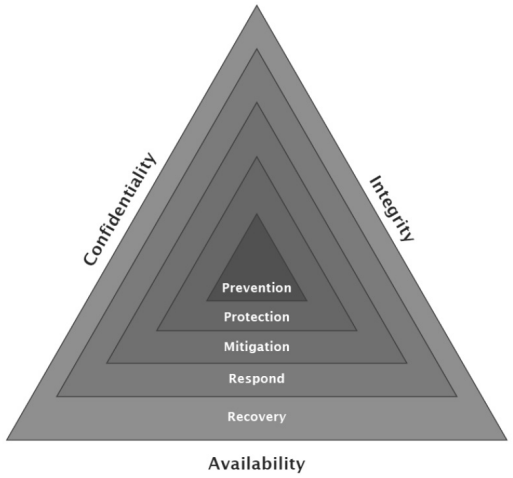


Figure 1: Conceptual framework on cybersecurity strategy

As illustrated in the framework, confidentiality, integrity and availability of data and information are goals of cybersecurity. The achievement of each of these goals can be enabled by a multi-layered approach to cybersecurity. In other words, prevention, protection, mitigation, respond and recovery measures can all be established in order to achieve confidentiality, integrity and availability respectively. Hence, in planning a cybersecurity strategy, one possibility is to work through each layer to identify corresponding measures needed to achieve confidentiality, integrity and availability respectively.

At the same time, the conceptual framework can also be used as a conceptual guide to evaluate cybersecurity strategy. A formulated strategy can be appraised against the framework by working through each layer and ensuring that adequate cybersecurity measures are incorporated within the strategy.

In using the framework, it will be useful to take note of two practical points. Firstly, users of the framework should be cognizant that each layer of the framework is an ideal type and overlap across the layers is fine. Hence, a single security measure may appear in more than one layer. For example, anti-virus software can appear in the integrity-prevention segment as it can scan for viruses and prevent a system from being infected. At the same time anti-virus software can also appear in the integrity-respond segment as it is able to clean up and remove the virus bug.

Secondly, not every layer needs to have corresponding cybersecurity measure. This is because there may not be any cost-effective measure available. However, when a particular segment is left blank, an assessment of the risk involved will have to be done and accepted by the management in alignment with the company's enterprise risk management.

Conclusion

Along with the growing interest in business analytics, businesses are amassing more data and using more information than before. At the same time, the dynamic nature of the cybersecurity landscape where new threats and counter measures are constantly evolving, the assurance of confidentiality, integrity and availability of data and information is also becoming more challenging than ever before. In view of these, businesses which adopt a multi-layered approach for their cybersecurity strategy will have a better chance in ensuring that the "New Oil" (i.e. data) that power their next stage of growth remains safe and secure.

Contemporary regulatory regime and intensifying cybersecurity threat landscape are also demanding business managers and executives to take on greater responsibility in ensuring cybersecurity. However, most business managers and executives are unfamiliar with cybersecurity concepts. The conceptual framework on cybersecurity strategy introduced in this chapter thus provides a primer in guiding business managers and executives to plan and evaluate their firms' cybersecurity strategy. This enables them to assume a larger role in the management of cybersecurity in their firms.

CHAPTER 8

CYBERSECURITY IN CORPORATE IT GOVERNANCE

Vincent Loy, PricewaterhouseCoopers

Introduction

The digital age provides immense opportunity for organisations to grow, develop and be more efficient, revolutionising customer, supplier and staff relationships and experiences. However, in seizing these opportunities, organisations can make themselves vulnerable to the very real and increasing number of evolving cyber threats. In addition to financial loss, organisations may suffer disruption of operations, destruction of key assets, loss of reputation and also loss of integrity and trust of products and services. Cyber risks are a clear and present danger to any business ecosystem. The threats are dynamic, broad and sophisticated - traditional approaches to security are too narrow and flat footed.

Many organisations still place the responsibility for managing cyber threats solely in the hands of their technology team. Traditional approaches to security that focus on compliance, technology solution in isolation, perimeter and back office based will not give the confidence to seize opportunities in today's digital, connected world. To effectively manage cyber risks, corporate organisation must be transformed from ones that are centered on security and technology to ones that combine these with business management, risk disciplines, and cyber threat expertise.

Cybersecurity as part of corporate IT governance

Managing cyber risk is a fundamental part of business management and business leaders need to see cyber threats for what they are – enterprise risk management issues that severely impact their business objectives. An appropriate cyber risk management programme should be one of many components of the organisation's IT governance process that covers the overall business risk environment that feeds into its enterprise-risk management framework.

Cyber risks should be treated like other serious business risk issues. To avoid potential damage to an organisation's bottom line, reputation, brand, and intellectual property, the Board and Management needs to take ownership of cyber risk. Specifically, they should collaborate up front to understand how the organisation will defend against and respond to cyber risks, and what it will take to make their organisation cyber resilient.

IT Governance is about the Board and Management responsibility for creating value for the organisation through IT and to align and manage the IT related risks, e.g. cyber risks. Since cyber risk can't be completely eliminated, the Board and Management need to decide on the level of cyber risk they are willing to accept, and then build their defenses around those parameters. By aligning with business needs, setting standards, and having better communications between IT and business users, organisation can effectively protect its most valuable assets and gain strategic advantages.

In light of the significant differences in each organisation's internal and external environment, there is no single IT governance model that is optimal. The key IT decisions, involvement of stakeholders, governance structures, processes and policies/principles/standards will be different for every organisation. The governance arrangements need to be flexible to change rapidly to address cyber risk management issues (Exhibit 1) and as factors in the internal and external environment changes.

Exhibit 1: Cyber risk management issues and best practice approach from leading organisations

Issue	Description	Best practice approach from leading organisations
Cyber threats viewed solely as an IT issue rather than a business issue	In most corporate organisations, cyber threats are managed by IT. However, in the new reality, the damaging consequences of poor cyber risk management spill over to impact the entire business.	Rather than having IT manages cyber risk, leading organisations hold the CEO and Board of Directors accountable. Business lines and risk management play a key role in identifying and classifying information assets.
Lack of common processes and methodologies	A corporate organisation's threat-monitoring and analysis activities are often disjointed, (for example, spread across multiple locations, maintained by different internal and external organisations, and hosted on multiple systems). This inhibits the ability to gather and manage cyber risk intelligence so as to recognise and rapidly respond to new threats in an evolving cyber security landscape.	We see leading corporate organisations establishing programmes that integrate processes, technologies, and risk methodologies into an enterprise-risk management programme that manages cyber business risks in line with their risk appetite.
Cyber risk flying below the radar	While many corporations have processes and controls in place to manage day-to-day risks, they often do not address cyber risks. These two types of risk share similar traits; both are hard to quantify, seem remote, and have a low probability of occurring. Typically, data-security systems are designed to meet just minimum levels of regulatory or industry compliance, rather than to identify the risks to the business and implement appropriate safeguards. Such institutions are ill-prepared to anticipate cyber threats and prepare a response in advance. They can only react.	Rather than taking a defensive posture, leading organisations are being proactive in identifying, planning for, and mitigating the cyber business risks that are most likely to impact their organisation.

Inability to look at the big picture	Existing information-security monitoring is largely focused on identifying and reacting to cyber threats in isolation. Traditional tools are only capable of identifying specific unusual patterns or traffic types and alerting operational teams when something outside the norm is happening.	Leading corporate organisations are transforming their organisations from ones that are centered on security and technology to ones that combine these with business management, risk disciplines, and cyber threat expertise. As they become cyber resilient, the organisation is able to plan for, and mitigate, cyber risks according to its appetite to withstand disruption and financial loss.
Reluctance to share cyber security intelligence	When things go wrong, responses typically only address the specific problem at hand. Few attempts are made to see if similar problems are occurring in other parts of the organisation. Often, organisations' cyber defenses rely primarily on data generated by internal monitoring rather than by reaching beyond enterprise boundaries to share insights and experiences.	Leading organisations establish open communication channels between corporate security, information security, threat management and analysis, law enforcement coordination, intelligence agencies, fraud, and operational risk to facilitate timely sharing of threat information with the right people to help mitigate the impact of cyber-attacks.
Taking a one-size-fits-all approach	Many corporations do not consider the value of different assets when planning their cyber risk management strategy —making it difficult to set priorities regarding the investment of resources.	We have observed leading corporations building a cyber-risk management programme to protect their revenue streams, business processes, assets, facilities, brand, and reputation.

Approach in managing cybersecurity risk

In order to effectively manage cyber risks, corporations should adopt a cyber-risk management programme that allows to plan for, and mitigate, cyber risks according to their appetite to withstand disruption and financial loss. Effective implementation of the programme can help organisations position themselves to gain a competitive advantage over their more vulnerable competitors that have opted to stick with the status quo.

The cyber risk management programme should consider key questions included in Exhibit 2.

Exhibit 2: Questions to consider as part of a cyber risk management programme

- Have we performed a cyber business risk assessment to identify our key business risks?
- How do we know where to invest to reduces our cyber risks?
- What would be the disruption to our business from a cyber attack? How would it affect our business, brand, and reputation?
- How much revenue would we lose if our business processes were impacted by a cyber event?
- Have we identified our most critical business assets and do we understand their value to our adversaries?
- Have we looked at the value of these assets and business processes through the lens of the various threat actors?
- Do we have a cyber incident capability that will allow us to quickly respond to a cyber attack?
- How do we establish cyber risk tolerance to the organisation?
- How do we communicate about cyber risk to the Board and other stakeholders?
- Is my business resilient enough to survive a cyber attack?

An organisation's cyber risk response should be ongoing and iterative. The programme should evolve as the organisation gains more insight into the nature, scope, and location of threats, and garners a better understanding of what it needs to protect and how. The steps to implement a cyber risk management programme (Exhibit 3) are as follows:

1. Establish cyber risk governance.
2. Understand your cyber organisational boundary.
3. Identify your critical business processes and assets. This step involves leveraging cyber insurance options, and upgrading cyber security technologies.
4. Identify cyber threats.
5. Improve your collection, analysis, and reporting of information.
6. Plan and respond. This step includes developing playbooks, improving cyber intelligence gathering techniques.

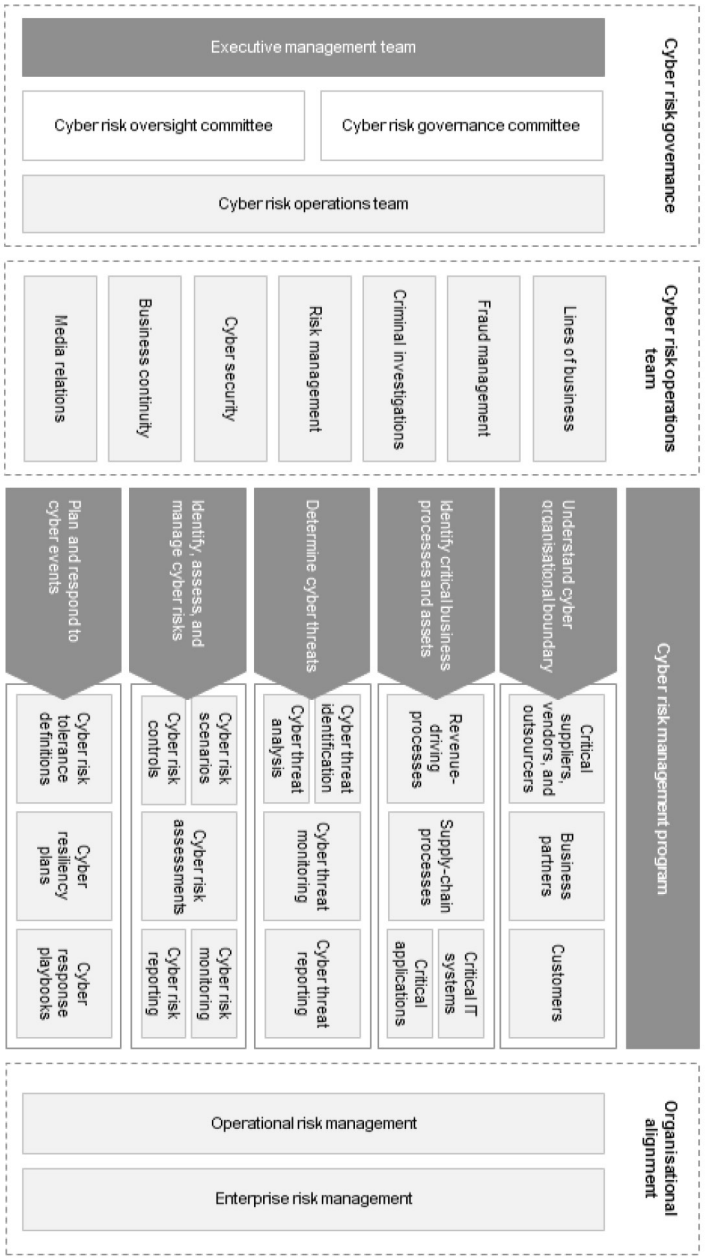


Exhibit 3: Framework for a cyber risk management programme

1 **Establish cyber risk governance** – The foundation of a strong cyber resilient organisation is a governance process for managing cyber risks. This is established by deciding who will be on each of the teams, and setting up operating processes and a reporting structure. Connections should also be made to other risk programme such as disaster recovery, business continuity, and crisis management.

Group	Key players	Responsibilities
Cyber risk governance committee	• Chief Operating Officer (COO) • Chief Risk Officer (CRO) • Head of Security • Heads of businesses and functional areas (such as business continuity planning, legal, risk/regulation)	• Works with senior leaders to develop cyber risk strategy. • Decides which information assets are essential. • Sets budget for cyber risk. • Monitors the organisation's cyber risk position and reports on it to senior leaders and the board of directors. • Reviews reports from the cyber risk oversight and operations teams and helps prioritise emerging cyber threats. • Revisits strategy to adapt the programme as the cyber risk landscape evolves.
Cyber risk oversight committee	• Information technology team • Business support team • Business teams	• Assesses the active risks the organisation faces, the people behind them, and the assets they threaten. • Evaluates the effectiveness of the operations team. • Identifies new threats and improves how information assets are protected. • Determines how business changes affect the cyber perimeter — including new service offerings, suppliers, vendors, or business partners. • Monitors status of patches and configuration changes to critical systems. • Oversees employee training programme. • Reviews new regulatory and compliance requirement.
Cyber risk operations team	• Managers with operational experience of networks, information security, fraud, and corporate security • Security operations center	• Acts as first line of defense for detecting and responding to cyber events. • Compiles real-time information from all the groups that monitor cyber threats. • Produces reports for the cyber risk oversight and governance committees, including items such as: number and type of cyber events, origination and duration of events, which assets have been targeted, kinds of fraud attempted, comparison of cyber events to industry trends, incident and response reports, threat assessments, and intelligence reports.

2 **Understand your cyber organisational boundary** – An organisation's cyber vulnerabilities extend to all locations where its data is stored, transmitted, and accessed — by employees themselves, its trusted partners and its customers. Organisations should also consider new areas such as big data, analytics, and social media.

Any weakness in the perimeter becomes the organisation's vulnerability. This challenge will only increase as the organisation's cyber security perimeter continues to expand as customers increase their demands for mobile tools that allow access to their information from wherever it resides to wherever they may be.

Key steps	Key considerations
Develop an enterprise level view of where critical assets and data reside	• Putting equal priority on all of the data that the organisation generates is not practical, cost effective, or necessary. Some of it is insignificant, but some is mission critical and will cripple the business if exposed. • Organisations should determine where their critical data stores are, where they are located at any given time, and who has access to them. This information can help develop a network perimeter. In addition to cloud, the evolution of big data, analytics, and social media have caused the boundary to be revisited.
Determine what systems and networks it traverses in supporting business operations	• The perimeter extends far beyond the typical corporate network boundary to trusted business partners, outsourced data centres, customers, and the cloud.
Understand all the data shared with business partners, third parties, and "fourth parties" (third parties' data outsourcing and partnership arrangements)	• Organisations should ensure they have the means and capability to have transparency into the cyber organisational boundary that extends far beyond the areas they directly control to wherever their critical information, data, and facilities reside. Any weakness in the perimeter becomes your vulnerability. • Organisations should enhance pre-employment due diligence for any insider who will have responsibility for IT operations, access to sensitive and protected data, responsibility for electronically transferring money, and other vulnerable functions.

3 **Identify your critical business processes and assets** – Organisations should determine what comprises their most valuable revenue streams, business processes, assets and facilities. We refer to these collectively as "crown jewels." After these are identified, understand where they are located and who has access to them. Asset classification is not a new concept, but many corporations still struggle to get it right — organisations are over-protecting some assets and under-protecting others.

Key steps	Key considerations
Identify critical assets and important business processes	• Crown jewels are those information assets or processes, which if stolen, compromised, or used inappropriately would render significant hardship to the business. • Examples of crown jewels may include trade secrets, market-based strategies, trading algorithms, product designs, new market plans, or other business processes in addition to information assets.
Determine value of each asset and business process to the organisation	• A "one-size-fits-all" model doesn't apply when protecting key information. Corporate organisations should hold business executives accountable for protecting the crown jewels in the same manner as they are accountable for financial results.
Define risk tolerance levels	• Corporate organisations should define the right level of risk tolerance for their organisation based on their business type. This will help determine the level of protection needed given their identified values and related risks.
Establish the levels of protection required for each asset type	• This would also include defining the ownership of risk for each asset, and establishing who within the organisation can make decisions on accepting or mitigating risks related to them. • Corporations can then prioritise their assets based on business risk.

4. **Identify cyber threats** – Existing information security monitoring identifies and reacts to cyber threats in isolation. Most information security tools are designed and implemented to identify specific unusual patterns or traffic types and alert operational teams that something outside the norm is happening. The responses address little more than the specific problem at hand and are often quickly forgotten. Few attempts are made to see if similar problems are occurring in other parts of the organisation or if others are experiencing the same threats.

   Effective cyber risk monitoring focuses on building a sustainable and resilient approach to putting intelligence inputs from various functional teams together under a common lens to quickly correlate and dynamically adjust the risk posture of the organisation to these threats in real time.

Key steps	Key considerations
Bring together the various teams responsible for managing, tracking, and responding to cyber events	This should include the following: • Internal security operations center (SOC): IT operations team, systems for security information and event management (SIEM), and incident-response teams. • Cyber risk governance: cyber risk governance committee, cyber risk oversight committee, and cyber risk operations team. • Cyber threat intelligence can also provide valuable information to groups responsible for detecting fraud, money laundering, and terrorism financing.
Adjust cyber risk and control posture of the organisation	• Adjust approach and perimeter as needed, depending on the location of assets, threat incidence, and state-of-the-industry landscape. • Refine and update processes as necessary to adjust to evolving cyber risk landscape.

5. **Improve your collection, analysis, and reporting of information** – Most organisations' threat analysis efforts inhabit a disjointed environment spread across several functions, physical locations and systems. This disjointed nature and lack of common methods to consume intelligence is a significant barrier to establishing a robust cyber risk intelligence capability. To close this deficit, organisations should establish a robust threat analysis capability that is built on shared intelligence, data and research from internal and external sources.

   To build a robust cyber intelligence infrastructure, corporations should ensure their cyber risk operations team supports the organisation by correctly analysing cyber risk data, providing leadership with the cyber risk information it needs to make informed decisions, and proactively and quickly responding to attacks.

Key steps	Key considerations
Analyse cyber risk data	• Work out where threats are coming from, when they're happening, and what tools the attackers are using. • Combine patterns you see from this analysis with knowledge of the business to give you a clearer picture of the threats you face. • Tailor your monitoring systems, dedicating more resources where needed, and tuning them to react more precisely to the threats you face. • Speed — both of processing cyber intelligence and reacting to it — is essential for combating the growing cyber threats you face.
Report to leadership	• Produce timely and meaningful reports for leadership, such as: the number and type of cyber attacks, the origination and duration of these attacks, which assets have been targeted, the types of fraud attempted, a comparison of cyber events to industry trends, incident and response reports, threat assessments, and cyber intelligence reports.
Proactively respond	• Take planned and rehearsed preventative measures to cyber attacks to shorten their duration and reduce the damage to the organisation.

6 **Plan and respond** – A strong governing team, with the right level of knowledge, expertise and involvement at all levels of the organisation, is required to appropriately respond to cyber events. But waiting to prepare your response until the cyber event has occurred is a recipe for disaster. The team must thoroughly understand the risks to their organisation, the tools at their disposal, and their options in responding before a cyber event occurs.

The development of prepared responses — playbooks — is a necessary step in adequately planning and preparing responses to cyber events. Using the intelligence gathered throughout the playbook development process, each playbook says who should take action, what their responsibilities are, and exactly what they should do.

There are five steps for developing these playbooks:

Key steps	Key considerations
Devise scenarios	• Think about the biggest cyber risks to your business and develop scenarios for some of the ways in which they're likely to happen. Each scenario should focus on a particular type of cyber attack and the assets it threatens. The scenario should also include the effects on your reputation, customers, finances, and your position with regulators.
Mitigate the effects	• Decide which processes, tools, and techniques would be available to deal with the effects of the cyber attack in each scenario.
Develop incident response plans	• What should your people do if an attack happens? Think about the people who own the information under threat. Also, consider each different part of the business — including corporate communications, media affairs, public relations, legal, marketing, law enforcement, and information technology. Write down the actions they should take, step by step, to get the business back to normal as quickly as possible.
Decide what extra resources you need	• Define what you need to have ready — people, tools, or equipment — to deal with the effects of the cyber attack in each scenario.
Rehearse	• Finally, get everyone to practise the responses set out in the playbook for each scenario. This gives people experience in dealing with cyber-attacks, and makes them less disruptive and damaging. Having a documented, practiced response to each kind of attack will make your organisation much more cyber resilient.

As the cyber risk management programme matures, executive management should revisit playbooks, revise cyber intelligence gathering techniques, leverage and update cyber insurance options, and upgrade cyber security technologies.

Conclusion

Cyber risk is no longer simply an IT challenge. As businesses become more completely dependent on technology and connectivity, the business impact of cyber attacks, affecting intellectual property, competitive advantage, operational stability, regulatory compliance, and reputation cannot be undermined. To anticipate and dynamically react to various cyber risks, organisations must establish a cyber risk management programme that has an ongoing capability to provide insight and intelligence on the cyber risks facing the business. Cyber risk management programme is important to reduce potential harm to the organisation's business and improve its cyber resiliency. It requires direction from business-operations leadership at a level that can commit and command the resources required to address and respond to cyber threats. An effective programme is a pivotal part of the business model and will position the organisation to take greater advantage of future business opportunities as they arise.

Case study 1

A Fortune 500 wealth management company noticed a spike in reported instances of online fraud related to its retirement savings plans. Several customers reported that their accounts had been taken over by hackers. The perpetrators arranged loans against the savings in these accounts and wired the amount of the loan to a third-party bank account. Using phishing and spear phishing schemes, the attackers succeeded in obtaining the account holders' personal login details.

The wealth management company adopted a cyber risk management programme and conducted an in-depth forensic analysis of the cyber incidents. The Management of the company implemented extensive changes in its approach to cyber security. The approach included:

- Establishing cyber risk governance which consists of executives from business and IT.
- Performing a computer forensics investigation that involved collecting more than 10 terabytes of digital evidence relating to these cyber incidents, including Web server logs, firewall logs, and intrusion-detection system logs.
- Analysing log data using Online Behaviour Analysis Tool. This enabled the company to determine which IP addresses and browsers the criminals used and what actions they took after gaining illegal access to customer accounts.
- Assessing the business impact of the cyber attacks, including identification of defrauded customer accounts and the source of fraudulent access. This helped to assess the legal risks it faced due to the privacy breach, and also enabled it to share crucial evidence with law enforcement.
- Developing playbooks that include the necessary steps in adequately planning and preparing responses to cyber events.

After the establishment of the cyber risk programme, the company had a better understanding of how the security breaches had occurred. It was also able to enhance its ability to detect and respond to cyber fraud by implementing a series of significant changes in its use of technology. The company also developed long-term, sustainable strategies to combat online fraud, including the development of an in-house incident response process.

Case study 2

The audit committee of a USD$1.9bn listed global business with operations in Asia was concerned that the threat of a cyber attack to their business was not consistently understood across all its operating units.

The company decided to establish a cyber risk governance process and develop a cyber crisis exercise that could be delivered in any territory. The objectives of the exercise were to raise awareness and provide assurance that local management were ready to respond when a cyber attack occurred. In conducting the exercise, the company ensured that local management understood the reality of the risk, were given a chance to rehearse their response in a safe environment, and develop cyber awareness.

A toolkit that delivered a realistic cyber scenario in each business location was developed. This included media news clips and mock webpages and required minimal changes prior to each exercise. The exercise also included performance of a penetration test, including social engineering attacks targeting general staff, at each location to identify staff awareness issues and security vulnerabilities in the security architecture and demonstrate the reality of the threat to each business.

As a result of the exercise, the management in each business unit developed a greater understanding of their exposure to cyber attacks, their risk profile and capability to respond. They also understood the level of maturity in cyber security and response capability across the business units, helping them target resources appropriately and improve preparedness for a cyber attack.

Having been through a rehearsal they were better prepared for a genuine attack, which did occur 18 months later.

CHAPTER 9

ANALYTICS IN CYBERSECURITY

Lyon Poh & Lee Ser Yen, KPMG in Singapore

Introduction

Cybercrimes are notoriously difficult to investigate and prosecute, which has in turn emboldened cyber criminals. The actors of cyber attacks have evolved from techies, to governments jostling for control of the cyberspace, right down to criminals who have found a new playground.

Attacks have also increasingly become more sophisticated and organised, and there have been allegations that some governments have funded the development of tools and methodologies deployed in some attacks.

Ranging from advanced sophisticated malware like the Uroburos[1] malware to large scale distributed denial-of-service (DDOS) attacks with traffic volumes exceeding 100Gbps[2], these malicious attacks have destroyed or stolen intellectual property, and even crippled critical operating functions and interrupted revenue stream.

The odds are stacked against defenders. Modern day breach detection tools employ a variety of new technologies like sand-box to sieve and filter out potentially malicious code before they reach the organisation's infrastructure. These tools, in turn, have prompted attackers to develop corresponding counter-measures, such as anti-sandboxing malware.

[1]http://www.techweekeurope.co.uk/workspace/russian-intelligence-uroburos-malware-140494

[2]https://threatpost.com/large-scale-ddos-attacks-continue-to-spike/107254

Cyber defence requires prior intelligence

Traditional approaches to cybersecurity may have been effective in the past, focused on perimeter defence with signature-based detection tools. These may now fall short when it comes to defending against new breeds of attacks. Malicious codes that are able to circumvent signature-based detection tools are easily available to resourceful attackers. These malwares are often designed to exploit previously unknown vulnerabilities in popular software on their victim's computers.

Even after these vulnerabilities are discovered and reported, it usually takes months, including much testing, before a patch is released by software vendors and actually deployed in an organisation. This delay is probably even worse in organisations that do not have sufficient expertise and resources.

The key challenge in detecting the presence of malicious software lurking in an IT system is to be able to reliably differentiate it from legitimate activities. While viruses and worms are designed to disrupt or disable IT systems and services, most cyber attacks are stealthy and insidious. These attacks rarely generate much "noise". The malicious codes are designed to quickly acquire legitimate user rights and stay "below the radar" to avoid detection. Once they have gained privileged access rights such as database administrative access, it is only a matter of time before these codes locate confidential and sensitive data stored on databases and in protected folders.

What makes defending a cyber attack pernicious is that an attacker only needs to discover one vulnerability or weakness to succeed while the defender must guard against all possible threats at all times. The attacker has the advantage of time and space to look for the weakest link in the defence, in addition to the anonymity provided by the Internet. This asymmetrical "warfare" places an onerous demand on the resources of the defender who must be on guard and alert all the time. The defenders' task appears even more hopeless in organisations whose IT systems spread across multiple geographical locations, and are connected to a multitude of business partners and suppliers.

Analytics can play a role in a response

Tools such as security information and event management (SIEM) allow organisations to consolidate data from multiple security devices into one system. Many organisations have invested substantially in infrastructure to store event log information as part of their regulatory compliance efforts. Some are even tracking and keeping records of their full network traffic to detect behavioural anomalies such as sudden downloads of unusually large files.

However, SIEMs are only effective when installed in an environment with sufficient staff and appropriate processes to support investigation and analysis. More often than not, such systems suffer from having too much data, but too little analysis and actionable insights for the cyber defender to work with. Eventually, most of the data collected are simply archived.

The advent of sophisticated data analytics tools and affordable computing power with cheap storage is opening up new possibilities. While attackers may change their tools and approaches, their modus operandi remains the same. This behavioural consistency enables analytics technology to detect malicious attacks in a more timely and accurate fashion. Going beyond signature-based or even static defence approaches, these systems take into account user profile, behavioural and even business norms to establish the comparative baseline and flag out anomalies.

Such an early detection system to sieve out probable threats as quickly as possible goes a long way to contain any potential damage.

What is Analytics?

Analytics is the process of drawing meaningful patterns and insights from data.

Beyond providing an explanation for an occurrence, analytics can be used to predict patterns and thereby help businesses plan pre-emptive actions. The real value of analytics thus lies in its insights, rather than hindsight.

Data analytics has been around for a long time, but it is the exponential growth of processing power and technology that has heralded in the era of 'Big Data'. The term is broadly used to describe data sets so large and complex that traditional data processing applications are inadequate. With technological advances and the rapid reduction of hardware costs, the colossal volume of security-related data that firms increasingly have to deal with can now be processed and analysed in a matter of minutes or even in real-time.

How can data analytics enhance cyber defence?

Traditional cybersecurity tools rely on pre-defined patterns and scenarios modelled from past known attacks to detect and block suspicious behaviours.

A good example is rule-based event correlations where some pre-existing knowledge of an attack is required to build a "precise" rule. This reactive approach can only identify known attacks, malware or viruses. New variants are likely to remain undetected until they are linked to a discovered breach.

Data analytics can map what normal daily behaviour looks like and flag anomalies, such as a computer that suddenly starts downloading unusually large files. Such statistical-based event correlations do not depend on pre-existing knowledge of any malicious activity but rely on the recognition of what represents 'normal activities'.

Modelling and linking

Using advanced mathematical models, the normal environment is modelled so that when activities deviating from the norm occur at a statistically significant range, these are flagged as high threat and trigger automatic defence mechanisms.

What constitutes 'normal' can be further broken down based on user profiles. Quite often corporate directories do not specify the profile of each user.

Using mathematical models, users are clustered based on multiple characteristics and a normal baseline is established for that group of users (Figure 1). Network behaviour that deviates from the cluster characteristics suggests irregularity and warrants investigation.

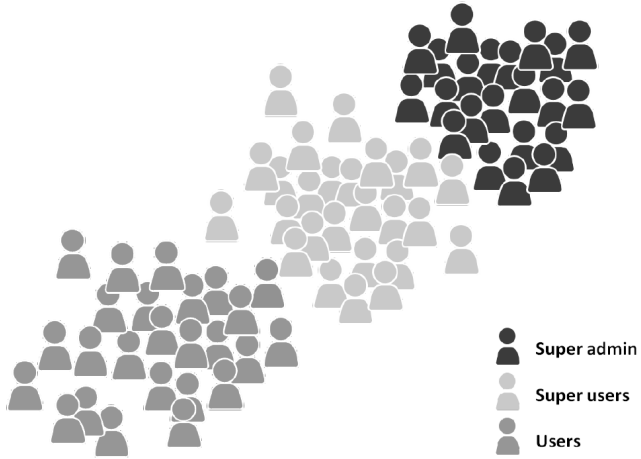


Figure 1: Clustered modelling

Link analytics, also known as graph analysis or process mining, works in a similar fashion. Data is modelled in the manner of a graph, where each node can represent a user, a server or an external IP. The nodes are connected to each other based on network requests and user activities. Different characteristics of these interactions are represented quantitatively such as the volume, frequency, time of day, or time distance between requests. Based

on this network graph which can be modelled in real time, suspicious activities can be identified and responded to. Figure 2 illustrates how link analytics works.

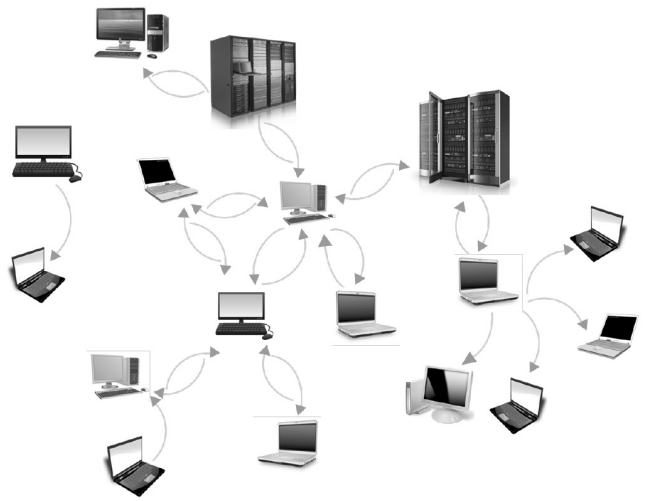


Figure 2: Link analytics

Such techniques are not new, but with the lowering of data storage and processing costs, it is now possible to derive meaningful insights in a very short time from such advanced computation intensive models.

Deploying analytics in cybersecurity

Cybersecurity is a process that constantly reacts to a dynamic threat landscape while catering to the changing needs of the organisation. Figure 3 illustrates the iterative process required to counter cyber threats and manage cyber risks actively.

- **Prepare** – Understanding and improving the organisation's current state of preparedness against cyber attack.
- **Protect** – Designing and implementing the organisation's cyber defence infrastructure.
- **Detect and respond** – identifying existing and potential attacker behaviours and their presence on the organisation's networks. Implementing a transparent cyber incident response plan.
- **Integrate** – Embedding cybersecurity in the culture and decision making of an organisation to help ensure it stays one step ahead.
- **Cyber threat intelligence** – Implementing the building blocks of intelligence and, in mature organisations, use intelligence as a springboard for delivering effective cybersecurity.
- **Cybersecurity transformation** – Organising and delivering a holistic programme of change to improve the organisation's cybersecurity capabilities.

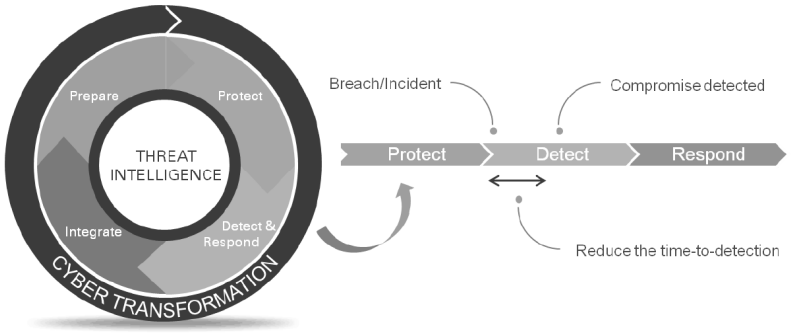


Figure 3: KPMG Cybersecurity framework

Preventive measures such as penetration testing, strengthening server configurations (server hardening), scanning for and removing known vulnerabilities should still be deployed to ensure the "hygiene" of cybersecurity.

However, such defensive measures alone are not sufficient. Cybersecurity analytics can improve situational awareness and potentially reduce the elapsed time between incident and detection. As an add-on to traditional cybersecurity defences, this field enhances cyber incident monitoring, investigation and analysis.

Figure 4 shows a high-level view of a cybersecurity analytics setup which is integrated into a security log collection and event monitoring system.

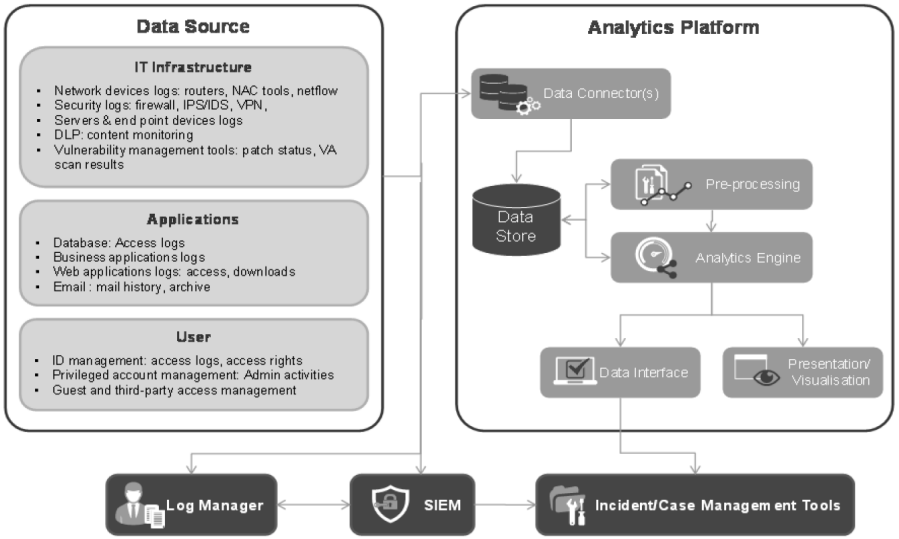


Figure 4: High-level view of a cybersecurity analytics setup

The key components of this will include:

Data source	Data is the key ingredient of an analytics setup. Sources of data types range from IT infrastructure, applications and user activities
Data store	Repository of data collected. Optimised for storage, retrieval and searching
Data interface	Allows integration with workflow engines for incident and case management
Analytics engine	Runs on computing infrastructure optimised for Big Data and Analytics workload
Presentation	Present information to analyst in various format, including 3D visualisation

Organisations can put this together themselves by using open-source components (e.g. Hadoop for data storage, Hive for analytics). A growing number of commercial-off-the-shelf products are also available to speed up deployment time.

Integrating the cybersecurity analytics setup with existing incident management (or case management) tool allows organisations to reduce false alerts and better manage their monitoring workload.

Strategy for deploying security analytics

The end goal of applying analytics to cybersecurity is to provide a comprehensive and timely view of the security posture of an organisation so that it can respond faster and better in the face of cyber attacks. Even better, pre-empt and neutralise such threats.

Cybersecurity is a journey, not a destination. Deploying cybersecurity analytics starts with investing in a system that will improve situational awareness, evaluate existing security monitoring capabilities and form the core of cyber defence activities.

Some key steps include:

- **Assessing how well the existing security infrastructure addresses security risks**. This can include identifying “blind spots”, capability and operational gaps
- **Determining if technology requirements can be met** by out-of-the-box analytics, or by bespoke solutions. The volume of security data collected, processed and stored may require new investments in computing power and storage
- **Assessing the expertise required** and whether there is a need for professional services
- **Establishing critical metrics** (e.g. time to discover a security incident, time to remediate and recover etc.) to measure the ROI of a security analytics implementation on security risk management targets

- **Starting off with an area where existing monitoring systems** can be enhanced with security analytics
- **Broadening data sets** to gain better insights. These can include event logs to network flows, system audit trails, packet captures, identity context, external intelligence feeds

Analytics in action

To better illustrate how cybersecurity analytics work, following are some examples of typical use cases.

Detecting anomalous behaviour

Outliers may suggest anomalous behaviour. By applying analytics to historical logs, the system can detect atypical behaviour patterns. Some examples include:

Administrator activities: When a system administrator account is compromised, it is sometimes accompanied by unauthorised user accounts created for future use. A correlation between this activity and a change in control system can be used as a red flag.

Unusual network connections: Each company has standard, fixed communication channels between clients and servers. Any aberrations from those patterns can signal that attackers are attempting to infiltrate other computers in the organisation to access sensitive information and move them to staging servers for 'exfiltration'.

System access inconsistencies

Attackers using stolen user credentials (ID and passwords) obtained by phishing or other means, are likely to log in from a suspicious (or unexpected) physical location. By geo-tagging login credentials, network traffic analysts can determine if login activities are legitimate. Any inconsistencies across login requests, such as logging in from different parts of the world within minutes, can also be used to flag unauthorised system access.

Anomalous data movements

Attackers who have successfully staged information on internal servers usually encrypt it into one large file or many small files, before transferring it to an external location. These locations are usually anonymous, and internet sharing sites that can be easily accessed from another location at a later time. Such activities can be detected by analysing data traffic and identifying any data, or specified thresholds of data volumes, moving from an internal server to an external site.

Conclusion

As cybersecurity analytics technologies and solutions are still evolving rapidly, it is important to recognise that utilising analytics involves a learning process. The setup needs to be reviewed and fine-tuned over time to enhance the outputs.

New data sources will constantly improve analysis and bring new insights and means of detection. It is prudent to start small with a subset of the data available while planning for a wider deployment.

Analytics enables organisations to derive deeper intelligence from their data-sets. When applied to cybersecurity, the actionable insights provided should allow them to detect and stop potential breaches faster and more efficiently. This is probably the decisive advantage cyber defenders need so as to prevail over increasingly determined attackers.

CHAPTER 10

CYBERSECURITY AS RISK MANAGEMENT

Gerry Chng, EY in Singapore

Over the last decade, the terms used to describe the activity of protecting digital assets have been changing. When organisations were still in the stage of infrastructure build-up, the focus was around protecting the IT infrastructure, and supporting infrastructure systems such as emails, domain name services, web sites and intranet applications. Such activities were conveniently labelled as IT security and it was usually the responsibility of the IT department to make sure that the right security settings were in place, and the systems were updated with the latest vendor patches.

Today, most businesses are heavily reliant on technology to run their business processes and reach out to their customers. As a result, there is a growing recognition that the intellectual property and customers' personal information available on these technological infrastructure are more valuable than the infrastructure itself. Some firms begin to use the term "information security" to signify that the focus should be on the information that drives the business. While the responsibility remained with the IT department, it has become more challenging as the IT Department is merely the custodians of the IT infrastructure that is owned and used by the business departments.

On 12 February 2013, US President Barrack Obama issued the Executive Order 13636 titled "Improving Critical Infrastructure Cybersecurity", which led to the widespread adoption of the term cybersecurity. The new term signifies the recognition of the increasing threats to the digital platforms from perpetrators over a digital channel. Such digital channels can be the networks, mobile applications, portable devices, cloud-enabled infrastructure, personal smart devices, or the Internet of Things.

While some may argue that this is just using a different term to describe the same activity, the use of the word "cyber" does capture the shifting reliance on digital technology. We have achieved sophisticated engineering feats such as power generation, water management, advanced coordination of transportation grids by combining traditional engineering fields with information technology. Consumers may make buying decisions based on product information obtained online. In our everyday lives, being connected 24/7 provides us with the information we need – directions, places to go, news, social media connectivity – to make impromptu decisions on-demand. These are just some examples of how our digital life has evolved with the consumerisation of digital technologies such as the ubiquitous Internet and smart device platforms.

Across the other side of the fence, the strategies adopted by hackers are also shifting from attacks of mischief to one that is much more targeted with a clear purpose within the secretive hackers' black market. Some parties in this black market provide the tools and services to obtain personal information or to break into systems. Others provide platforms for anonymous payments of such illegal activities, or provide servers that are either anonymous or in jurisdictions that make it close to impossible to locate and shut down these systems.

Arguably, hacking techniques have not changed much, ranging from discovery of vulnerabilities, to "weaponising" these into malware, phishing emails or social engineering attacks to trick a prospective victim. These remain the mainstay of hackers' approaches, which are known as Advanced Persistent Threats. What has changed now is that such attacks are now carried out with much more discretion, instead of casting a wide net as they did previously. By being more targeted and discretionary about what to attack, hackers avoid raising anomalies in detection systems that help security companies reverse-engineer their techniques and consequently lock them down.

Hackers recognise that, through such techniques, they can gain access to a wealth of valuable digitised information, which, when not properly secured, can be obtained online without needing to be physically at the enterprise. Insecure systems with customer information provide names, emails, and sometimes passwords that can be sold in the black market to fuel phishing email campaigns. These phishing email campaigns can be launched to gain access to a trusted employee's computer or create a network of compromised systems waiting for further instructions, either as a future target or being a participant in a botnet of compromised computers that can be used in Distributed Denial of Service attacks.

With intensifying cyber threats, it is little wonder that some have identified 2014 as the Year of the Data Breach as large organisations worldwide found themselves becoming targets of cyber-attacks.

To fight this trend, some organisations try to limit the content that can be made available online, or resist the adoption of innovative technology. However, organisations that adopt this approach take on a bigger risk of losing agility and ability to compete against more innovative companies that enhance the overall customer experience through technology.

Enterprise issue, not an IT problem

Amid the notable data breaches seen in 2014, a positive outcome is that such events have prompted Boards and Executive Management to question if their organisations are ready for such blatant attacks.

Yet, the questioning of their readiness does not translate into capabilities to deal with attacks. Organisations have expressed that they are not confident of their current capabilities in dealing with a targeted attack using sophisticated methods. In EY's recent Global Information Security Survey, Get ahead of cybercrime, 56% of respondents say that it was unlikely or highly unlikely that their organisation would be able to detect a sophisticated attack.

While there is the general recognition that cybersecurity is more than an IT problem, most organisations have not been taking a different approach to deal with the issue. IT management still focuses on simply implementing security products or demonstrating point-in-time compliance. This gets increasingly frustrating for Boards as they struggle to understand the effectiveness of security management. Lessons from past incidents have shown us that simply buying more security products, or demonstrating point-in-time compliance does not stop security breaches entirely.

Indeed, if one examines the mega data breaches in 2014, a majority of these organisations that have fallen prey to attacks have invested heavily in information security in the form of security solutions, certifications, or dedicated teams of security analysts. Yet hackers were able to slip through the technological, compliance, or process gaps. Even more disturbing is the long period of time that hackers stayed undetected after a successful breach. In a recent Mandiant M-Trends 2014 report, it is found that the median dwell time of a compromise before detection was 229 days, with the maximum dwell time being 2,287 days. That is nearly six years before the compromise was detected!

This brings an important question. Do organisations really know what hackers want, and the means through which they can achieve that? Are organisations keeping their eyes on the right areas as they invest in security solutions and resources?

To be fair, there are countless means through which hackers can achieve their objectives. While hackers just need a single gap to slip through, IT management needs to safeguard and monitor all possible entry points with limited budget and resources. The adoption of cloud-based and mobility solutions, along with an extended enterprise comprising of third-party vendors has exacerbated the situation.

Further, the traditional approach of relying solely on security solutions to stop all attacks has resulted in a flood of alerts with different priorities, making it difficult to decipher what is important. Thus, Boards and Executive Management find it difficult to extract useful insights on whether security initiatives are placed in the right areas.

This gap increases the tension between the IT Department and Executive Management, as there is still a disconnect between the way cybersecurity is communicated and how other enterprise risks are presented. The result is that cybersecurity remains an IT problem, and in the absence of meaningful indicators, a zero tolerance to successful cybersecurity breaches becomes a norm.

Taking a different approach

This expectation gap needs to be addressed with utmost urgency. Should the gap be left to grow, the likely outcome may be the adoption of technology without the right security foundations. This will result in a culture where the innovative use of technology is avoided. Risks and rewards from the adoption of technology are two sides of the same coin. While it is not advisable to reside on either extreme, it is necessary to take a balanced approach by harnessing the benefits of technology while avoiding risks that are beyond established tolerance level.

It is probably with this in mind that the National Association of Corporate Directors issued a Director's Handbook Series titled Cyber-Risk Oversight in 2014. The paper acknowledged that "if a sophisticated attacker targets a company's systems, they will almost certainly breach them." It also advised that "leading companies view cyber risks in the same way they do other critical risks – in terms of a risk-reward trade off."

The paper outlines five key principles to help organisations exercise their fiduciary responsibilities:

1) Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue;
2) Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances;
3) Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be featured regularly and at appropriate time interval;
4) Directors should set an expectation that management establish an enterprise-wide cyber-risk management framework with adequate staffing and budget;
5) Board-Management discussions about cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Boards and the Executive Management can help to close the expectation gap by requiring cybersecurity risks to be treated in a similar way as other enterprise risks.

If we look at how other forms of enterprise risks have been handled, it usually comprises the following broad categories of activities:

a) Clear definition of the activities and ownership;
b) Understanding of a list of possible risk scenarios;
c) Mechanism to rank the list of risks by its inherent and residual nature;
d) Definition of Key Risk Indicators (KRIs) to provide an early-warning indication;
e) Identification of suitable metrics and/or simulation models to monitor against KRI;
f) Maintaining a risk posture within established tolerance levels;
g) Defining a risk appetite statement as a high-level statement to guide management activities.

Approaches and techniques

For nearly a decade, technology management has been driven by legal, regulatory, or industry-specific compliance regimes. This has eroded sound technology risk management principles as organisations struggled to keep up with endless waves of audits and remediation activities, resulting in situations where they may be going through the routine to put in technology or processes without first understanding the fundamental threats.

Thus, it is important to establish robust technology risk management with the following components.

Clear definition of cybersecurity

In most matured organisations, technology risks have been incorporated as part of operational risks. The coverage of technology risks can be very broad and includes areas such as resiliency and availability, adoption of standardised enterprise architectures, obsolescence management, meeting regulatory expectations, and security management.

As these specialisations typically require different fields of computer science expertise, it is rare to find an individual sufficiently knowledgeable in all aspects of technology risks.

Cybersecurity risks can be defined as the realisation of threats from malicious perpetrators over a digital communication channel targeting a company's digital assets. The intentions may include theft, alteration, or disruption to the business.

Cybersecurity risk management involves the activities around proactively identifying, assessing, controlling, and monitoring such threats.

By having a clear definition of cybersecurity, it allows the organisation to ensure that skilled resources are available to focus risk management activities around threats to digital assets.

Establish right governance structures

A right governance structure aids in decision-making around how an organisation handles risk-reward situations presented by the adoption of technology.

The governance structure should be established at various management tiers with clear charters on the responsibilities and decisions to be made at each tier. It should also comprise a balanced senior management representation from business lines and IT to encourage the right conversations around cybersecurity risks and rewards. This also helps to ensure that the business risk owners are fully cognizant of the issues and their responsibilities.

Establish an integrated risk management framework

Organisations should integrate their cybersecurity risk management with enterprise risk management activities. This helps to instil a consistent method of identifying, analysing, treating and monitoring risks. By using the same language and risk ratings, it allows cybersecurity risks to be elevated for Board and Executive Management discussions alongside other enterprise risks.

An effective cybersecurity risk management requires a risk-initiated approach to assessing risks, rather than the traditional security compliance or checkbox approach. While the latter is still needed to test IT systems and applications against desired baselines, it should not be the only mechanism on which the risks are assessed. The main issue with relying on a compliance approach is that not all risk scenarios may be identified. In a typical compliance-approach review, risk scenarios are articulated in a manner that describes certain inadequacy in the security controls. Hence, there is a possibility that a risk may not be highlighted if the security controls are found to be adequate as specified by the risk scenarios.

Instead, a risk-initiated approach starts by identifying a list of possible risk scenarios that might result from the adoption of technology or process. At this juncture, the key objective is to derive a list of cybersecurity risks as complete as possible given the expertise present.

The benefits from adopting such an approach include:

a) A prioritised list of risk scenarios can be identified with a risk profile to represent the technology initiative;

b) The controls selection can be specific for the risk scenarios identified;

c) Key metrics can be designed to test whether the important controls are operating as intended on an on-going basis;

d) A metrics-driven, trends-based approach can be adopted as early-warning indicators to alert management that risk thresholds are close to the defined tolerance levels;

e) Such representations can also be used in conversations with Boards, Audit Committees, and Executive Management to provide the assurance that the right level of due diligence has been established.

This integrated risk management framework provides a platform for Boards and Executive Management to drive the necessary change to deal with the increasingly sophisticated threat landscape.

Adopting an objective controls environment

Organisations should also incorporate a centralised risks and controls library as part of this framework. This allows subsequent risk assessments to be performed consistently and objectively, and enables a model to be developed to compute the residual risk ratings based on the application of controls.

There are numerous libraries that can be considered, such as the ISO 27002 standards and the NIST SP 800-53 list of controls. Organisations can adapt such standards into their risks and controls library in the initial creation of their library.

Security awareness programme

In many organisations, it is not difficult to find users who use weak passwords, use the same password across different applications, or will be tempted to click on a link in an email. These users may actually be adopting a lower level of security control than is required by the organisation's cybersecurity policies. In today's interconnected world, hackers are increasingly targeting such users as a conduit to get to their ultimate target by first compromising the workstations, smart devices, or cloud services of these users and subsequently navigate the organisation's network to get to their ultimate target. Thus, it is important that everybody in the organisation is kept informed of such emerging threats and be cognizant that they may be prime targets for hackers. This security awareness outreach should be engaging and not just another compliance exercise, and should also be targeting at all levels including Senior Management and external vendors who have access to the organisation's assets.

Organisations are also increasingly engaging in unannounced tests to gauge the effectiveness of their security awareness programmes. These include controlled phishing email attacks on staff and vendors, or the deliberate leaving of portable storage devices preloaded with controlled executables. Other than being used as a gauge of the programme's effectiveness, it is a deterrent as staff and vendors become more conscientious when they face similar situations.

Cyber insurance

In the wake of the data breaches, victims are faced with direct financial losses resulting from breach notifications and the costs of restoring the environment.

This has sparked an interest to transfer part of the risks attributed to the direct financial impact through cyber insurance. While this is a viable option, organisations should be mindful that such policies will only take care of part of the direct financial losses. There can be potential losses arising from the reputational and regulatory impact that will not be sufficiently covered by these policies.

Media outreach programme

In today's social media world, it is also important to have the right response prepared prior to an actual breach. One of the most damaging responses towards a successful hack is to keep completely silent about the issue while customers and the public engage in speculation on social media. Such uncontrolled speculations can become viral in a very short time and has the potential for a huge impact on the organisations' long-term reputation. Such damages can also be difficult and costly to reverse.

Technology to put it all together

With the establishment of the right framework, it provides a platform for IT Management to identify and measure risks objectively and consistently. It also allows key metrics to be presented as trends that can be used in conversations with the Board, Audit Committee, and Executive Management on the on-going risk posture.

Three notable technology initiatives should also be considered to bind the activities together. These are an automated Governance, Risk, and Compliance Solution to make the processes more efficient; Identity Access Management Solution to more effectively manage digital identities; and a Security Operations Centre to consolidate the security mechanisms and ensure a dedicated team is monitoring the threat landscape.

Governance, risk, and compliance solution

With the complexity of the information and coordination required in the risk management techniques described above, it is not feasible to perform these risk management activities using spreadsheets and emails. Organisations should consider using automated solutions to streamline the risk assessment activities that are being performed.

Automated solutions have matured in the market over the last few years, with several large vendors providing tried-and-tested solutions that have been adopted by global organisations. A well-architected solution combines the people, process, and technology aspects of risk management activities to bring about enhanced visibility, consistency, and efficiency. This becomes key in making sure that the framework is achievable and becomes embedded in the organisation's DNA through the management of key metrics.

Identity access management solutions

In nearly all attacks, more often than not, the Achilles heel is the poor management of digital identities. This can arise from unnecessary accounts lurking in the IT systems, or users being granted excessive access privileges. Manual user recertification programmes exist in many matured organisations, but such methods are usually compliance-driven and managers find it difficult to reconcile an ID to an actual individual. The cryptic role definitions also make it difficult for managers to decipher the actual access granted to the IDs.

There is growing interest among organisations to adopt an identity and access management or governance solution, with several global vendors providing such solutions. These solutions help organisations create the digital roles and access matrix within systems, and aids in the consistent provisioning, modification, and de-provisioning of user identities during an employee's lifecycle.

Security operation centre (SOC)

The key controls identified should be managed by a dedicated team that focuses on watching activities as they are happening to identify and respond to potential security events. Depending on the size of the organisation, this can either be built and operated in-house, or outsourced to managed-SOC providers.

By having a dedicated team with the right technology enablement, it reduces the time needed to detect and respond to a potential breach. Combined with the definition of important key metrics, it ensures that the right resources are watching the right indicators at all times.

Conclusion

It is no longer prudent to hope that one may never be hacked. In today's evolving threat landscape, it is almost a certainty that a hacker will succeed in finding a loophole if the incentives are strong enough.

The question that begs an answer is, do we know what the hacker wants, and will we know when they have penetrated into our system? It is thus important to take a risk-initiated approach to anticipate as much as possible the scenarios in which a breach might occur. Combined with a strong identity and access management solution as well as security operations centre capability, the organisation can strive to reduce the time lapse between the breach and detection to limit the potential damage arising from a successful attack.

Such is the connected world we live in today. One that is full of potential, yet one where we are still constantly learning how to operate in safely and responsibly.

Disclaimer
The views reflected in this article are the views of the author and do not necessarily reflect the views of the global EY organisation or its member firms.

CHAPTER 11

CYBERSECURITY: THE CHANGING ROLE OF AUDIT COMMITTEE AND INTERNAL AUDIT

Siah Weng Yew, Thio Tse Gan, Kenneth Leong, Tan Ing Houw, Diona Lim, Deloitte Singapore

Introduction

Among the most complex and rapidly evolving issues companies must contend with is cybersecurity. With the advent of mobile technology, cloud computing, and social media, reports on major breaches of proprietary information and damage to organisational IT infrastructure have also become increasingly common, thus transforming the IT risk landscape at a rapid pace.

International media reports on high-profile retail breaches and the major discovery of the Heartbleed security vulnerability posing an extensive systemic challenge to the secure storage and transmission of information via the Internet have shone a spotlight on cybersecurity issues. Consequently, this has kept cybersecurity a high priority on the agenda of boards and audit committees.

- Organised crime is monetising cyberspace, exploiting vulnerabilities in computer systems to compromise and remotely control computers; recording key strokes, monitoring screen displays and manipulating the computer user into divulging sensitive data.
- Cyberspace being borderless allows any attacker to route their assaults through multiple countries and jurisdictions, complicating investigation and law enforcement.
- Companies run the risk of losing substantial amounts of sensitive company information to malicious employees, who could also potentially remove it from company premises or introduce malicious software to corrupt company databases or sabotage network operations.
- Corporate espionage by firms is commonplace in cyberspace. Attacks often target sensitive intellectual property, and there have been multiple instances of major firms with its security compromised over many months and losing substantial amounts of sensitive data during these attacks.
- Activism is also prevalent in cyberspace with sabotage and denial of service attacks growing progressively frequent. In the past, they would be attributed to 'hacktivist' groups such as Anonymous; but increasingly attacks point to political motivations.

Based on the Global Risk Landscape 2014 published by the World Economic Forum, cyber-attacks are one of the risks with high impact as well as high likelihood.

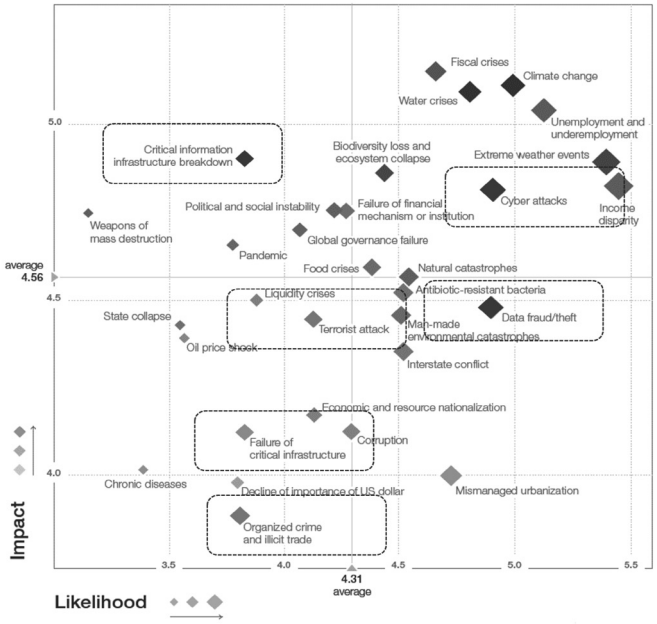


Figure 1: 2014 Global Risk Landscape (World Economic Forum)

What is the role of Internal Audit and the Audit committee?

a) Three Lines of Defence Model

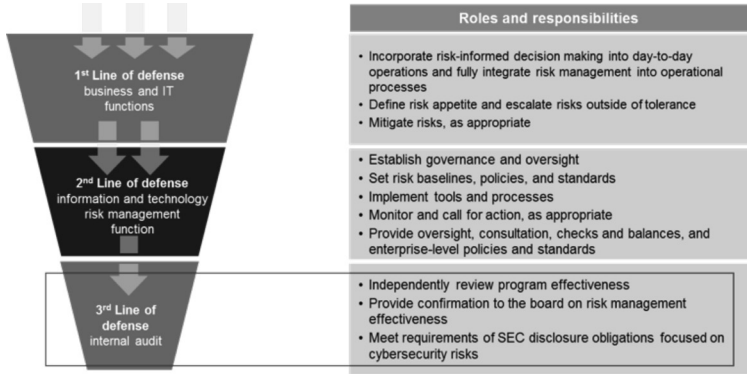
Effective risk management is the product of multiple layers of risk defence. Internal Audit should support the board's need to understand the effectiveness of cybersecurity controls. Organisations should institute and continually shore up three lines of defences:

1. **Management.** Companies that are good at managing information security risks typically assign responsibility for their security regimes to the highest levels of the organisation. Management has ownership, responsibility and accountability for assessing, controlling and mitigating risks.

2. **Risk management and compliance functions**. Risk management functions facilitate and monitor the implementation of effective risk management practices by management, and help risk owners in reporting adequate risk-related information up and down the firm.

3. **Internal audit**. The internal audit function provides objective assurance to the board and executive management on how effectively the organisation assesses and manages its risks, including the manner in which the first and second lines of defence operate. It is imperative that this line of defence be at least as strong as the first two. Without a function that provides competent and objective assurance, a company faces real risks of its information privacy practices becoming inadequate or even obsolete. This is a role that internal audit is uniquely positioned to fill. But to do so, it must have the mandate and the resources to match.

The three lines of defence illustrated below are not unique to data privacy and security, but should be in place and operating at a robust level to deal with any critical risk to the business. For most organisations, information security and privacy are critical risks because of its potential to cause financial and reputational damage.



Given recent high profile cyber-attacks and data losses, and the expectations of the SEC and other regulators, it is critical for Internal Audit to understand cyber risks and be well prepared to address the questions and concerns expressed by the audit committee and board.

b) Organisational roles and responsibilities for cybersecurity

Audit committee and board of directors — Overseeing a successful cybersecurity programme requires frequent and proactive engagement from the board of directors and audit committee. The audit committee, in its capacity of overseeing risk management activities and monitoring management's policies and procedures, plays a significant strategic role in coordinating cyber risk initiatives and policies and confirming their efficacy. These responsibilities include setting expectations and accountability for management, as well as assessing the adequacy of resources, funding and focus for cybersecurity activities. The audit committee chair can be a particularly effective liaison with other groups in enforcing and communicating expectations regarding security and risk mitigation.

Boards are devoting increased attention and resources to responding to cybersecurity issues. In a recent study[2] of global enterprise security governance practices conducted by the Carnegie Mellon University CyLab, 48 per cent of corporations surveyed reported having a board-level risk committee responsible for privacy and security risks, a dramatic increase from the 8 per cent that reported having such a committee in 2008. Among North American respondents, 40 per cent indicated that their company's board deals with computer and information security issues.

Whether or not there is a dedicated risk committee on the board, it is important to confirm that there are directors with knowledge and skills in security, IT governance and cyber risk. Given the audit committee's responsibility for risk oversight, it can be advantageous to recruit committee members with cybersecurity experience so that informed decisions are made about the sufficiency of the efforts overseen.

Management — All members of management should be fully aware of the plan of action and who will occupy key roles in the event of an attack or threat. Most companies have a senior management position related to information security in place so that there is a clear voice directing cyberthreat prevention, remediation and recovery plans, related educational activities, and the development of frameworks for effective reporting. This position is sometimes held by a chief information officer, or a chief security officer who is also responsible for physical security, but some companies may have a dedicated chief information security officer who focuses solely on cyberthreats. These executives will sometimes report directly to the board, but in all cases, they can be an effective liaison with whom the audit committee and board can communicate regarding risks and the response to attacks.

Internal audit — The audit committee should confirm that the internal audit function regularly reviews controls pertaining to cybersecurity, is up-to-date on the latest developments and include related issues prominently and regularly on its agenda.

External auditor — The external auditor can often be a valuable source of information on cybersecurity issues. Many firms have practices focused on evaluating and strengthening security controls and implementing programmes for enterprise risk management. They are also qualified to provide perspectives gained through working with a wide variety of companies in diverse industries.

External specialists — It can be helpful to seek the input of external specialists in assessing cybersecurity. Companies can conduct annual external reviews of security and privacy programmes, including incident response, breach notification, disaster recovery and crisis communication plans. Such efforts can be commissioned and reviewed by the board's risk committee or another designated committee to confirm that identified gaps or weaknesses are addressed. Third-party security assessments can also provide benchmarking relative to other companies of similar size or in the same industry.

c) The audit committee's role in cybersecurity

The extent of the audit committee's involvement in cybersecurity issues varies significantly by company and industry. In some organisations, cybersecurity risk is tasked directly to the audit committee, while in others, there is a separate risk committee. Companies for which technology forms the backbone of their business often have a dedicated cyber risk committee that focuses exclusively on cybersecurity.

Regardless of the formal structure adopted, the rapid pace of technology and data growth, and the attendant risks highlighted by recent security breaches demonstrate an increasing importance in understanding cybersecurity as a substantive, enterprise-wide business risk.

Audit committees should be aware of cybersecurity trends, regulatory developments and major threats to the company, as the risks associated with intrusions can be severe and pose systemic economic and business consequences that can significantly affect shareholders.

Engaging in regular dialogue with technology-focused organisational leaders will help the committee better understand where attention should be concentrated.

Some questions for audit committees to consider asking the management regarding cybersecurity are:

- What is the overall strategy and plan for protecting assets?
- How robust are the organisation's incident response and communication plans?
- What are the organisation's critical assets and associated risks to be secured?
- How are vulnerabilities identified?
- How are risks disclosed?
- How are critical infrastructure and regulatory requirements met?

- What controls are in place to monitor cloud and supplier networks, as well as software running on company devices, such as mobile devices?
- What digital information is leaving the organisation, where is it going, and how is it tracked?
- Do we have trained and experienced staff who can forecast cyber risks?
- Is it known who is logging into the company's network, from where, and if the information they are accessing is appropriate to their role?

d) Transforming cyber defences

Within the broader context of responsibility for risk oversight, audit committees are responsible for the oversight of financial reporting and disclosure, and more recently cybersecurity.

Cybersecurity is a business issue as it exceeds the boundaries of IT and cyber risk needs to be managed with as much discipline as financial risk.

Both the technical nature of the threat and amount of attention cyber risk demands calls for primary audit committee involvement. Yet organisations have acknowledged a lack of expertise on cybersecurity issues. As a result, audit committees are seeking not only education for themselves, but also an elevation of the discussion amidst C-level executives. These efforts include increasing engagement with the chief information officer (CIO) and chief information security officer (CISO), drawing on the expertise of the IT partner from the external audit firm, encouraging CIOs and CISOs to participate in peer-group information sharing, and challenging management to produce metrics that the audit committee can use to evaluate cybersecurity effectiveness.

A comprehensive cybersecurity plan also requires appropriate culture and tone at the top. These encompass an awareness of the importance of security extending from the C-suite to the professionals in each function, since breaches can occur at any level and in any department.

The CEO should make it clear that cybersecurity is a major corporate priority, and should communicate that he or she is fully on board with enforcing compliance with policies and supporting efforts to strengthen infrastructure and combat threats.

Several practices that companies are employing to enhance the audit committee's oversight of cybersecurity risk, leverage the recent broader strategic focus of the CISO and CIO roles:

1. Increasing interaction with the IT department

CIO and CISO should attend audit committee meetings and take the audit committee through one "deep dive" education session on cybersecurity issuse. The audit committee should also continue engaging with the CIO and CISO.

2. Sharing information with industry counterparts

CIOs and CISOs benefit from sharing information with their industry counterparts about cyberattack patterns and cyberdefence strategies. For instance, providing first-hand experience of a cyberattack to industry peers would better inform and prepare them for the prevention of similar attacks and in the process isolate a high-impact and high-likelihood risk from crippling an organisation.

3. Technology experts joining the board

The lack of technology expertise is an issue that has to be recognised in boards today. With the average age of board members exceeding 50, there is often a lack of understanding of context as a CIO is briefing the board. It is, therefore, beneficial for the board to have a member with significant technology experience.

4. Engaging the expertise of the external audit firm

External auditors employ a variety of professionals that include cybersecurity experts. They are a great resource for providing an honest perspective on the organisation – the knowledge of the management team and how the company is benchmarked. Some companies engage external audit firms to be "ethical hackers" without the knowledge of the CIO and/or CISO, while others choose to notify these executives ahead of time

5. Deploying internal audit

Internal audit plays a central role in helping the audit committee oversee cybersecurity. The regular assessments conducted by internal audit play an important part in providing the audit committee with a comprehensive appraisal of the organisation's strength and weakness. Internal audit should also be able to develop a road map for the future dealing with various cyber risk issues and scenarios.

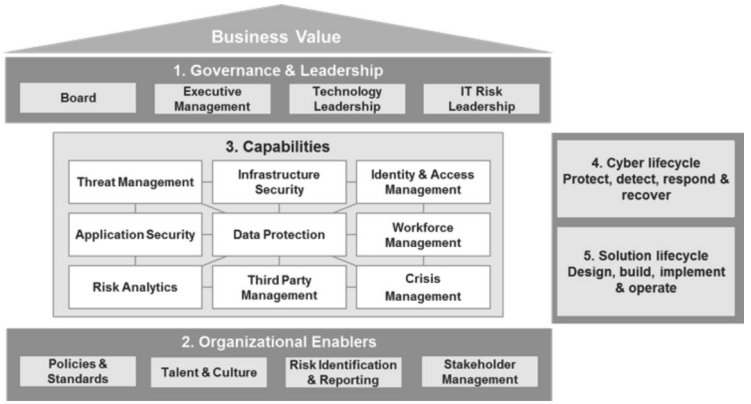
6. Evaluating the company's cybersecurity programmes

A company's cybersecurity programme can be difficult to evaluate because audit committees do not know the key success factors and its indicators to measure it. The most important indicator is the amount of time that elapses between the hacker's penetration and the company's detection. Detection and response time are among the most important metrics that the company should track to ensure progression and effectiveness of the techniques being employed.

Framework for Cyber Risk Management

The Cyber Risk Management Framework can help focus the conversation among the audit committee, other members of the board and senior management on what cybersecurity plans are in place and its possible gaps. This can potentially bridge the gap between the seemingly technical world of cybersecurity and how it translates into the governance decisions that boards and senior executives make. It also encourages dialogue between companies in similar industries which have a shared interest in identifying and addressing vulnerabilities.

The framework's core consists of five functions—governance and leadership, organisational enablers, capabilities, cyber lifecycle and solution lifecycle that provide a high-level, strategic view of an organisation's management of cybersecurity risks and examine existing cybersecurity practices, guidelines and standards.

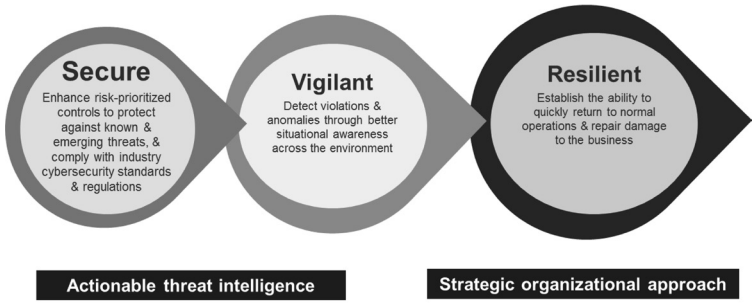


Cybersecurity plans should take into account the past, present and future with regard to cyber risks. Consideration should be given to the percentage of the available budget required for prevention efforts, immediate response to attacks and resiliency exercises.

Throughout the past decade, most organisations' cyber security programmes have focused on strengthening prevention capabilities based on established information assurance strategy: defence in-depth. This approach advocates a multi-layered approach to deploying security controls with the intent of providing redundancy in the event a security control fails or a vulnerability is successfully exploited in one of the layers.

To be effective and well balanced, a cyberdefence must have three key characteristics: secure, vigilant, and resilient.

1. **Secure:** Being secure means focusing protection around the risk-sensitive assets at the heart of your organisation's mission - the ones that both you and your adversaries are likely to agree are the most valuable.
2. **Vigilant:** Being vigilant means establishing threat awareness throughout the organisation, and developing the capacity to detect patterns of behaviour that may indicate, or even predict, compromise of critical assets.
3. **Resilient:** Being resilient means having the capacity to rapidly contain the damage, and mobilise the diverse resources needed to minimise impact - including direct costs and business disruption, as well as reputation and brand damage.



In summary, the above model has 3 objectives – secure, vigilant and resilient – woven together with 5 design principles of:

a) Incorporating security in the core design

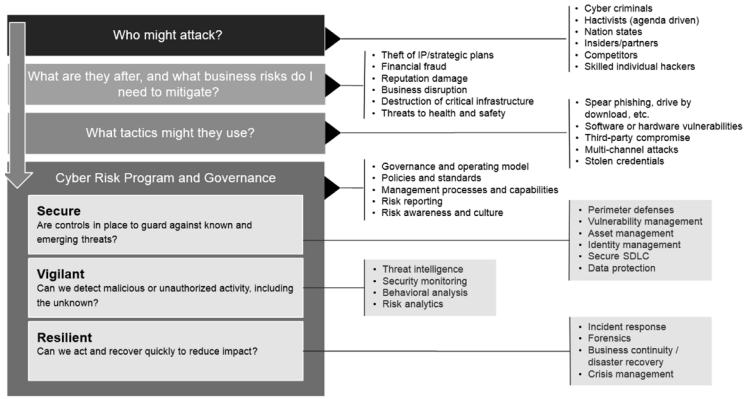
b) Applying threat intelligence in the core design

c) Sharing of intel and information among security practitioners

d) Automating processes to address the scarcity of skilled resources

e) Enabling the power of combating crime together

Once the cyber risks have been identified, the 3 objectives within the cybersecurity plan can be used to map the programme and governance to mitigate or address those risks.



Cyber risk appetite and tolerance

Risk appetite and tolerance must be a high priority on the board agenda. It is a core consideration in an enterprise risk management approach. Risk appetite can be defined as 'the amount and type of risk that an organisation is willing to take in order to meet its strategic objectives.

Every organisation possesses different risk appetites depending on their sector, culture and objectives. A range of appetites exist for a diverse portfolio of risks, which may change over time according to the risk portfolio. While risk appetite is interpreted differently, there is general consensus that effective communication of an appropriate risk appetite statement can help organisations achieve their goals and sustain their operations.

Management should develop an understanding of the cyber-criminal, their objectives, and how the attack might happen. The following questions can be used to develop the understanding:

1. Who might attack?
2. What are they after, and what business risks do we need to mitigate?
3. What is the intruder's arsenal?

A representative Internal Audit plan to address cyber risk

It is imperative that internal audit takes a leading role in determining whether a systematic and disciplined approach exists to evaluate and strengthen the effectiveness of cyber risk management. It should also determine if appropriate cybersecurity capabilities (people, process, and technology) are in place to protect against cyber threats.

In developing the internal audit plan for cybersecurity, the 2013 COSO Framework should be used as the framework for guiding the internal audit's approach. Managing cyber risk through a COSO lens enables the board and senior executives to better communicate their business objectives, their definition of critical information systems, and related risk tolerance levels. This enables others within the organisation, including IT personnel, to perform a detailed cyber risk analysis by evaluating the information systems that are most likely to be targeted by attackers, likely methods of attack, and points of intended exploitation. In turn, appropriate control activities can be established to address such risks. Through the COSO cube, organisations may view their cyber risk profile through the components of internal control to manage cyber risks in a secure, vigilant, resilient manner. For example:

Figure 2: The COSO Cube

a) Control environment — Does the board understand the organisation's cyber risk profile and are they informed of how the organisation is managing the evolving cyber risks management faces?

b) Risk assessment — Has the organisation and its critical stakeholders evaluated its operations, reporting and compliance objectives, and gathered information to understand how cyber risk could impact such objectives?

c) Control activities — Has the entity developed control activities, including general control activities over technology that enable the organisation to manage cyber risk within the acceptable level of tolerance to the organisation? Have such control activities been deployed through formalised policies and procedures?

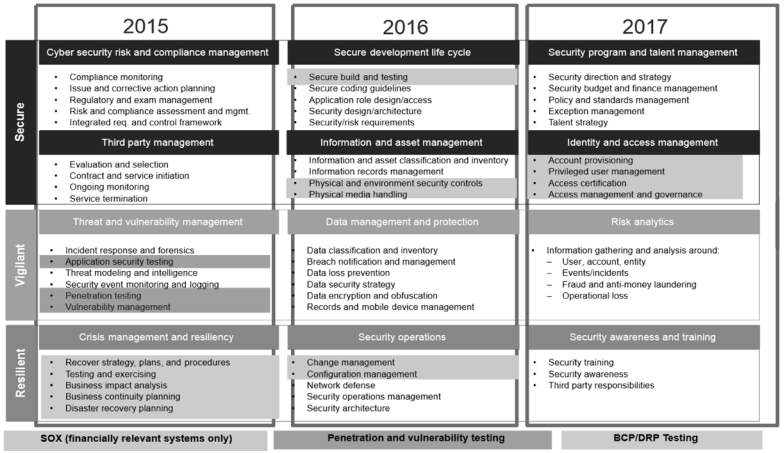
d) Information and communication — Has the organisation identified information requirements to manage internal control over cyber risk? Has the organisation defined internal and external communication channels and protocols that support the functioning of internal control? How will the organisation respond to, manage, and communicate a cyber risk event?

e) Monitoring activities — How will the organisation select, develop, and perform evaluations to ascertain the design and operating effectiveness of internal controls that address cyber risks? When deficiencies are identified how are these deficiencies communicated and prioritised for corrective action? What is the organisation doing to monitor their cyber risk profile?

A cybersecurity assessment can drive a risk-based IT internal audit plan, and audit frequency should correspond to the level of risk identified, and applicable regulatory requirements/expectations.

The following table illustrates the detailed cyber risk programme and governance derived from the three key characteristics (secure, vigilant, and resilient) linked to the internal audit plan each year to address the cyber risks.

Another approach is to allow some coverage of each area (Secure, Vigilant and Resilient) in each year.



Looking ahead

As recently as five years ago, it was rare for a board of directors to be closely involved in managing cybersecurity risks, but rapid advancements in technology, coupled with a corresponding increase in the sophistication of cyber criminals and cyber legislation, have made it essential for the board and audit committee to be informed and proactive. New technologies continue to shape the physical and virtual borders of organisations, which must frequently review and quickly adapt policies to address emerging issues.

Cybersecurity specialists are developing increasingly sophisticated approaches for preventing, detecting, and responding to security breaches, but no single solution can address all the evolving challenges associated with cyber threats. It remains important to apply prudent and adaptable controls to respond to changes in the threat landscape, and to have strong response and resiliency plans in place in the event of an attack.

Increasingly, cybersecurity is becoming a top-of-mind issue for most CEOs and boards, and they are becoming more preemptive in evaluating cybersecurity risk exposure as an enterprise-wide risk management issue, not limiting it to an IT concern.

CHAPTER 12

DIGITAL FORENSICS

Owen Hawkes & Eddie Toh, KPMG in Singapore

The reality of cyber crime today

Over the past decade, businesses have exponentially increased the volume of technology used across their organisations. From implementing Bring-Your-Own-Device ("BYOD") policies to private and public cloud computing, the shifting boundaries of technology and connectivity represent a critical vulnerability to those with malicious intent.

Cyber risks, in many respects, have not changed much in the last decade. Malware and phishing scams are not new, but organisations and individuals continue to fall victim to them as the sophistication of the attacks has evolved. We also see a shift in the targets of cyber attacks, from heavily invested IT infrastructure to employees, who are usually the weakest link in cyber defence. All it takes is one unguarded employee to click on an innocent-looking attachment for a phishing attack to succeed.

Digital evidence

Digital forensics is a relatively young discipline, but increasingly practised by law enforcement and private organisations all over the world. Digital evidence is now routinely presented in Court and used in the prosecution of all types of crime, not just computer-related offences. Digital evidence must be able to stand up to scrutiny of its provenance and interpretation. To be persuasive, it must be authentic, complete, reliable and believable.

Case study

External legal counsel to a listed company engaged us to analyse the computer system of a former employee. The company was concerned that the employee may have stolen its intellectual property shortly before joining a competitor. The data stored by the computer on its hard disk drive recorded the installation and deletion of file recovery applications, mass creation and deletion of files and folders, and copying of files and folders from the computer to external storage media. This could indicate that the former employee had been copying, deleting and recovering large volumes of data on the company computer. However, further investigation revealed that these activities were in fact undertaken by the company's IT department and the external legal counsel in an attempt to recover and extract information of interest from the employee's computer. In the process of doing so, not only was the integrity of the data residing on the computer system compromised, evidence was overwritten and rendered irrecoverable.

The nature of digital evidence presents a new set of challenges for investigators. Digital evidence:

- Is intangible in nature, i.e. cannot be viewed directly
- Is volatile and thus easily lost or destroyed, such as information in a computer's memory
- Is susceptible to manipulation
- Can be located in any data storage mechanism, which may not be in the same country as the investigation
- Requires the use of specialised computer technology to examine.

It is one thing to know that vital evidence is 'in there'. It is another to extract it in a useful, useable and admissible form.

Digital forensic procedures

Digital devices can retain precise records of activities, in more ways than is typically realised. Analysis, such as file and operating system analysis, can provide investigators with a wealth of information that may otherwise be inaccessible including hidden files, deleted files, partial file data and the ability to reconstruct files.

Whereas following the money may lead to a single perpetrator, digital forensics can explain the involvement of a whole gang, helping the investigator identify and prove, amongst other things, deliberate diversions of business, intellectual property theft, identify theft, and the misuse of a business's resources. Equally importantly, digital forensics can also indicate the innocence of suspects, often without the same level of publicity or reputational damage that conventional investigation can cause.

Digital forensics allows investigators to locate, preserve, and recover digital evidence in a defensible fashion, often for use in commencing or defending lawsuits. Throughout the process, the continuity of evidence needs to be maintained, with source data secured and original media preserved from use or interference in analysis. Figure 1 illustrates digital forensic procedure.

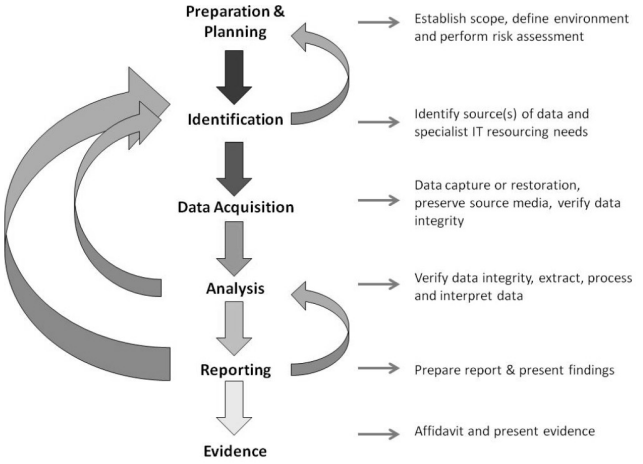


Figure 1: Digital forensic procedure

The **Preparation and Planning** phase focuses on defining the objective and scope of the investigation as a whole and any digital forensic procedures in particular, as well as identifying and resolving non-technical issues that may inhibit the successful completion of the procedures. Some considerations include:

– What is the focus of our investigation?

– Is this a covert or overt investigation?

– What are the resources (e.g. legal counsel, Human Resources personnel, IT personnel and forensic specialists) required to perform the investigation?

– What are the regulatory or legal obligations surrounding the investigation?

During the **Identification** phase, the focus is on identifying relevant sources of digital evidence, as well as any specialised IT skills and resources that may be needed to secure and extract the data. Some of the considerations are:

– What are the relevant sources of digital evidence?

– Where are the relevant sources of digital evidence located?

– Do you have the authorisation to take custody, preserve and analyse the digital evidence?

The **Data Acquisition** phase centres on data-gathering, where potential sources of digital evidence are captured and preserved in an evidentially sound fashion. Some of the considerations are:

– What type of documentation is required to maintain records of handling the Exhibit so that the "chain of custody" is unbroken?

– What are the resources and forensic tools required to preserve the original media?

In the **Analysis** phase, the acquired data is analysed for electronically-recorded facts that are relevant to the objectives of the investigation. Today's computer environments allow for the storage of virtually any document, transaction, or record. Common types of data analysed include:

– Office documents such as spreadsheets, text files and presentations

– E-mails (including web-based e-mail services such as Hotmail, Yahoo and Gmail), text messages, instant messages, and other electronic correspondence

– Financial records, including databases stored by common accounting systems, such as SAP and MYOB

– Address books, calendars and journals

– Internet browsing history and internet cache files

– Files uploaded and downloaded using Cloud platforms, such as DropBox or OneDrive

– Temporary files and auto-recovery files generated by programmes such as Microsoft Word

– Records of recently accessed folders or files on shared folders or external devices

– Deleted files and fragments of files from unallocated disk drive space and virtual memory

– Windows registry information, such as programmes installed and used

– "Metadata", i.e. information about how and when data has been created, deleted accessed and used.

In the **Reporting** phase, the procedures undertaken in the Identification, Data Acquisition and Analysis phases are summarised and findings are provided in a report. Some of the considerations for the report's authors are:

– Who will be reading the report?

– Should it be written in technical or layman's language?

– Does it contain the facts and analysis to support the report's findings?

– Are the findings in the report capable of being supported by the Identification, Data Acquisition and Analysis phases if evidence is required for a trial?

The nature of forensic work demands that we assume from the outset that findings from an investigation may be offered as evidence in legal proceedings. In the **Evidence** phase, evidence offered by a witness is normally limited to personal experience and, if that person is acting as an "expert" witness, the opinion of that person in respect of a relevant aspect of the proceedings. The evidence provided by a witness must be unbiased and objective.

Case study

A major multinational company suffered an exodus of employees from a commodities trading department, prior to them joining a competitor. Suspecting that something was amiss, senior management instructed the company's IT personnel to secure and quarantine computer systems assigned to these employees as at their last day of work.

Using specialised forensic technology hardware and software, we created exact copies, called "images", of the hard disk drives on the computer systems. This enables the data to be analysed on the copies of the hard disk drives and prevents damage or loss of evidence on the originals. Analysis of data on the images showed that information had been deleted, formatted or wiped using commercial wiping software. The presence of such software is often considered suspicious on its own.

However, other critical information was uncovered from the remnants of files found on the hard disk drives. Such data is harder to destroy; indeed not all users of computers know that it remains even after deletion of files. This data included deleted instant messenger conversations, SMS and webmail correspondence. These provided evidence that the mass walkout was incited by certain employees. The computers also recorded files containing the company's proprietary information being downloaded by some of the employees.

This information enabled the company to obtain a Court order to search the residences of the former employees without warning, and to obtain further computers, digital storage media and physical documents for analysis.

Cyber attacks

From simple malware that disables an employee's mouse to sophisticated Advanced Persistent Threats, the range of cyber threats has grown rapidly, and preventive measures necessarily trail behind.

The information security market is huge. In 2014, organisations around the world spent US$71bn on information security. While cyber attacks that are featured in news headlines often focus on theft of customer data, other attacks precisely target intellectual property or material disruption of the targeted business for extended periods.

Risks arise from a number of failings, including poor security policies and procedures, misconfiguration of IT systems, malicious actions by trusted insiders, or external network intrusion.

Some of the most common cyber attack types today are:

- Phishing or spear-phishing
  An attempt to fraudulently acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by email and often directs users to enter details at a fake website.
- Man-in-the-Middle
  A form of cyber attack where electronic communication (such as emails) between two users is intercepted by a malicious actor. This actor then retransmits the message while replacing the requested key with his own. The two original parties still appear to be communicating with each other, when in reality, the entire conversation is controlled by the attacker. Figure 2 illustrates a man-in-the-middle attack.
- Advanced Persistent Threats (APT)
  A network attack in which an unauthorised person gains access to a network and undetected for a long period of time. The purpose of an APT attack is to steal data rather than to cause damage to the network or organisation.

- Ransomware

  A type of malware which prevents or limits access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.

- Distributed denial of Service (DDOS)
  This happens when a large number of compromised systems attack a single target, overwhelming it with traffic from multiple sources and thereby causing denial of service for users of the targeted system. Victims of DoS attacks often target web servers of high-profile organisations such as banking, commerce, and media companies, or government and trade organisations

Case study

A major beverage company did not receive the expected full payment of an outstanding amount from a distributor in the region. The company and the distributor had worked together for several years and built a trusted relationship. Both companies mainly corresponded through email. While the company used a registered email domain, the distributor used a free web-based email service.

A few weeks prior to the payment cycle, the company and the distributor received email instructions from a purported member of staff informing them of a change in email addresses. This individual had created false email addresses for various staff both in the company and at the distributor and sent fictitious emails to each group confirming the changes of email address. By doing so, the perpetrator became a "man-in-the-middle", monitoring and responding to emails of both the company and the distributor.

Email correspondence appeared to be "business as usual" until the payment cycle began. The perpetrator then instructed the distributor's staff to split the payment into two sums, some to the company's real bank account and the remainder to the account of a purported subsidiary.

The instructions were followed and payments were made. Only weeks later did the distributor become suspicious when asked to make further payments to the "subsidiary" bank account.

Digital forensic investigation revealed that computer systems used by the staff of both companies were infected with malware. This malware allowed the perpetrator to obtain information such as the login details for the web-based email accounts and other confidential business information. By becoming a man-in-the-middle, the perpetrator intercepted email correspondence to monitor business activities between the two companies to identify when and how to execute the fraudulent scheme.

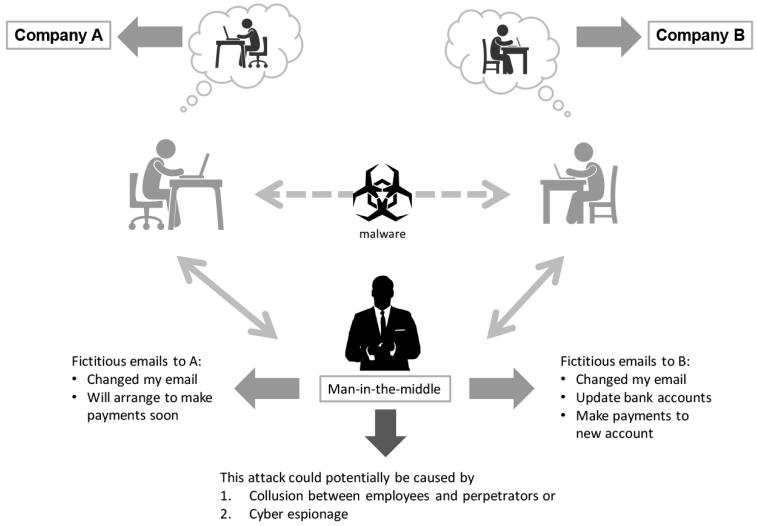


Figure 2: Man-in-the-Middle attack illustration

Responding to cyber attacks

An incident response plan outlines the steps that companies should take in the aftermath of a security breach. The goal is to mitigate the breach by minimising damage and reducing recovery time and costs from such an incident.

Figure 3 shows an incident response process created in accordance with internationally accepted frameworks, including the National Institute of Standards and Technology Special Publication 800 86 (NIST SP800 86), the International Organization for Standardization (ISO) publication 18044:2044, and the SANS institute's published Six Step Incident Response Process (SANS 6 Step IR). It consists of six phases:

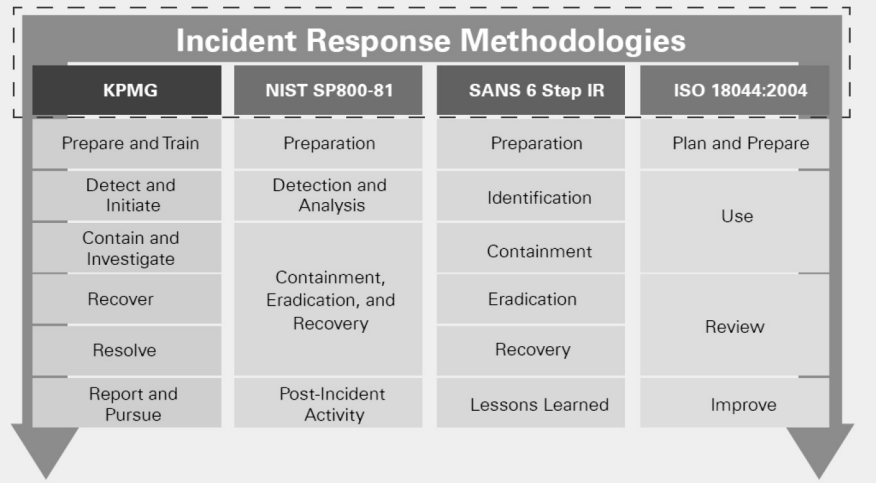


Figure 3: Incident response process

Prepare and train - one of the most common causes of a poor response is a lack of adequate preparation. An incident response team should be prepared to conduct a comprehensive and objective internal investigation by having available and understanding clear lines of communication and response protocols. This allows an incident response team to gather facts, assess the impact of the incident, and to adopt the best course of action without having to invent procedures in the midst of a crisis.

Detect and initiate - the trigger for this phase is an alert, an indicator of fraud, or a communication from an outside entity, such as law enforcement or an Internet service provider. The incident response team should be able to provide swift answers to pressing questions, such as "Have we been breached?", "Is the activity continuing?", and "What is the potential damage?"

Contain and investigate - during this phase, the incident response team determines the source, method, and impact of the security event, while attempting to minimise damage. These efforts are typically a balancing act between investigating and eradicating the threat. Responses can range from allowing the malicious action to continue in order to facilitate evidence gathering to an immediate suppression of malicious action in order to limit damage.

The task is to manage damage while being cognizant of the potential that a useful evidence trail may exist. If an attack is still in progress, there exists the possibility of tracing the attack to the source. If the attack is no longer active, it is essential to close the vulnerability to prevent further intrusion or incidents. In general, the type of cyber incident will determine the steps to be taken in this phase. Phishing, man-in-the middle, APTs, ransomware and DDOS attacks have different considerations and priorities. For example, in the event of a data breach, the incident response team should consider the following:

- Are there regulated data at risk?
- Are there business sensitive data at risk?
- Are there customer data at risk?
- Is the press or public aware of the incident?
- Is a notification procedure to a stakeholder or regulator required?

Regulators are taking tougher stances on data breach notification. In the US and Europe, organisations are required by law to report breaches, and to notify individuals if the security of their personal data is compromised. In Singapore, the Monetary Authority of Singapore requires banks to report IT security incidents within the hour.

Recover - this phase consists of efforts to remove the threat that could not be undertaken during previous phases because of the potential impact on investigative efforts or prioritisation of other activities. The focus of this stage is to return the IT environment to normal operation. During the recovery phase, assessing what was lost and whether data was copied, removed or modified is critical. If files and databases were removed, this phase would involve restoring them to their last known state.

Resolve - a significant element of this phase is vulnerability assessment and penetration testing. This work may occur concurrently with other aspects of the incident response process, and should be followed by a detailed process to determine the root causes of the malicious activity. This phase is aimed at improving the technical and governance environments, which can help prevent similar events from occurring in the future.

Report and pursue - the final phase consists of reporting to the appropriate stakeholders and may include ongoing support activities related to criminal or civil suits against individuals or entities.

Advanced tools and techniques

The advancement of technology has made cyber attacks more complex and more difficult to detect. A 2014 report by Mandiant, a cyber security consultancy, suggested that most breaches are only detected after a median average of 205 days after the attack commenced.

To tackle these attacks, forensic investigators require advanced tools that can cover ground quickly, examine data in great depth and identify threats accurately. First responders without the required tools are unlikely to be able to react to cyber attacks effectively. Beside employing and training specialists, investing in tools is crucial.

Conclusion

Cyber crimes and attacks are becoming increasingly common in this region and are likely to increase. An organisation can mitigate the risks posed by cyber attacks by investing in people, technology and cyber governance. However, regional organisations' IT security is still relatively unsophisticated.

Companies should assume that their IT infrastructure will be compromised at some point and ensure that they are prepared to detect and respond to cyber incidents when they happen. An understanding of digital forensic principles will help investigators identify and obtain vital digital evidence. The early application of digital forensic procedures can aid investigations, as well as enabling a better understanding of the threat faced.

ABOUT THE EDITORS AND AUTHORS

Editors

Dr Gary Pan is Associate Professor of Accounting (Education) and the Associate Dean for Student Matters of the School of Accountancy at the Singapore Management University. He is currently a Fellow member of CPA Australia, a Chartered Accountant of Singapore, and Certified Management Accountant of Australia. Before the SMU appointment, Gary was Senior Lecturer of Accounting at the University of Melbourne, Australia. His teaching and research interests are Accounting Information Systems, Fraud Prevention & Internal control and Business Analytics. Gary has published over 50 papers in academic refereed journals and conferences. He is Associate Editor for Journal of Information & Management and also author of the book "Dynamics of Governing IT Innovation in Singapore: a Casebook".

Dr Seow Poh Sun is Associate Professor of Accounting (Education) and Associate Dean (Teaching and Curriculum) of the School of Accountancy at Singapore Management University. Prior to joining SMU, Poh Sun was a lecturer at The University of Melbourne and worked in PricewaterhouseCoopers Singapore. Poh Sun received his PhD in Accounting from The University of Melbourne and obtained his Masters of Business Administration and Bachelor of Accounting with First Class Honours, both from Nanyang Technological University. His teaching and research interests are in accounting information systems, behavioural issues in accounting and accounting education. Poh Sun has won a number of international and local teaching and research awards. Poh Sun is a Fellow member of CPA Australia, a Chartered Accountant of Singapore and a member of American Accounting Association, European Accounting Association and Accounting and Finance Association of Australia and New Zealand.

Dr Calvin Chan is the Vice Dean of the School of Business at SIM University (UniSIM) and a Visiting Professor in the e-Government Innovation Centre at the University of Brunei Darussalam. His research interest is in the organisational and social aspects of information systems, especially information systems in the public sector. He is a board member of the Council for Third Age, a member of the Silver Industry Standards Committee (SISC) under the Singapore Standards Council and Chairman of SISC's Technical Committee for Technology. He is on the Editorial Board of the International Journal of Intercultural Information Management. He has also served as the Deputy Convener of the Cloud Security Working Group under the Information Technology Standard Committee. Dr Chan graduated with a BSc (HON) in Computer and Management Science from the University of Warwick and a PhD in Information Systems from the National University of Singapore. He has previously worked for the Infocomm Development Authority of Singapore on the Infocomm Security Masterplan.

Dr Lim Chu Yeong is currently an Associate Professor of Accounting (Practice) with the School of Accountancy Singapore Management University. He has 15 years of industry experience, in treasury, financial accounting and management accounting positions primarily within the financial sector. His finance and accounting experience span major companies including Credit Suisse, Citibank, Shell, Standard Chartered Bank, the Government of Singapore Investment Corporation (GIC) and the Development Bank of Singapore (DBS). His latest position prior to joining SMU was VP at Credit Suisse. Chu Yeong has taught Intermediate Financial Accounting, Advanced Financial Accounting and Valuation. He has published in reputable journals such as Journal of Accounting and Public Policy. He holds a PhD from Manchester Business School and a MBA from the University of Warwick. He is a member of CPA Australia and a Chartered Accountant of Singapore.

Contributing Authors

Calvin Chan, Vice Dean, School of Business, SIM University

Gerry Chng, Partner, Advisory Services at EY in Singapore

Sean Dunphy, Director, Deloitte Analytics

Owen Hawkes, Partner, KPMG in Singapore

Sidarth Khashu, Director, EY in Singapore

Lawrance Lai, Partner, EY in Singapore

Lee Ser Yen, Director, KPMG in Singapore

Lee Yew Haur, Head, Business Analytics Programme, School of Business, SIM University

Kenneth Leong, Director, Risk Consulting, Deloitte Singapore

Diona Lim, Assistant Manager, Clients & Markets, Deloitte Singapore

Vincent J Loy, Partner, Financial Crime & Cyber Leader, PricewaterhouseCoopers LLP

Judy Ng, Managing Director, DBS Bank

Gary Pan, Associate Professor of Accounting (Education) and Associate Dean (Student Matters), School of Accountancy, Singapore Management University

Tim Phillipps, Global Leader, Deloitte Analytics and Deloitte Forensic

Lyon Poh, Partner, KPMG in Singapore

Ananya Sen, Managing Director, DBS Bank

Seow Poh Sun, Associate Professor of Accounting (Education) and Associate Dean (Teaching and Curriculum), School of Accountancy, Singapore Management University,

Siah Weng Yew, Executive Director, Risk Consulting, Deloitte Singapore

James Tan Swee Chuan, Senior Lecturer, Business Analytics Programme, School of Business, SIM University

Tan Ing Houw, Director, Risk Consulting, Deloitte Singapore

Tan Shong Ye, Partner, PricewaterhouseCoopers LLP

Thio Tse Gan, Executive Director, Risk Consulting, Deloitte Singapore

Eddie Toh, Director, KPMG in Singapore

CPA Australia
1 Raffles Place
#31-01 One Raffles Place
Singapore 048616

+65 6671 6500
sg@cpaaustralia.com.au
cpaaustralia.com.au

SMU School of Accountancy
60 Stamford Road
Singapore 178900

+65 6828 0632
accountancy@smu.edu.sg

SIM University
461 Clementi Road
Singapore 599491

+65 6248 9777
sbiz@unisim.edu.sg

Download a QR code reader on your smartphone and scan for a soft copy of this book.

ISBN 978-981-09-5560-1