# UK Security Breach Investigations Report

An Analysis of Data Compromise Cases

2010

Supported By

SOCA
SERIOUS ORGANISED CRIME AGENCY

PCeU
Police Central e-crime Unit

University of Bedfordshire

7safe®

# Preface

There are a great number of surveys in existence that demonstrate the rise in information security breaches, their associated costs and current practices. These include, but are not limited to, the DTI Information Security Breaches Surveys (see, for example, [1,2,3, 4], and the ninth and most recent survey [5] , surveys from the Ponemon Institute (see, for example [6], [7], [8] and [9]), and surveys from the European Network and Information Security Agency (ENISA) such as the Current Practice and the Measurement of Success report of July 2007 [10]. This latter report features the data reported by 67 companies across Europe with only 12 being interviewed in depth.

However, some of the problems of using surveys as a reliable source are obvious. Most notable is that when using self-reporting, there are a number of factors that influence the level of accuracy in the data that a company reports. This, combined with the fact that the data presented is that reported by a sample of companies, leads to disclaimers regarding the use of the data and subsequent inferences. It certainly would seem to contradict modern understanding of business when the 2008 Information Security Breaches Survey published by the Department for Business, Enterprise & Regulatory Reform [11] states in its preface that it "is encouraging to see that information security incidents are causing less disruption to companies' operations than two years ago." It is fully understandable that some businesses will simply not wish to go on record stating the accurate size or cost of a breach unless legislation forces them to. Equally, there may be companies that are simply unable to calculate the size or cost of a breach.

This report, rather than relying on questionnaires and self-reporting, concerns cases that were investigated by the forensic investigation team at 7Safe. Whilst removing any inaccuracies arising from self-reporting, the authors acknowledge that the limitation of the sample size remains. It is hoped that the unbiased reporting by independent investigators has yielded interesting facts about modern security breaches.

**Published January 2010**

This report may be downloaded in electronic format from
**www.7safe.com/breach_report**

# ABOUT THE AUTHORS

Professor Carsten Maple holds a chair in Applicable Computing at the University of Bedfordshire. He has undertaken numerous research projects in various areas of Computing and Information Security and has given talks to businesses and universities around the world advising on information security. He is an elected member of the Committee of the Council of Professors and Heads of Computing in the UK.

The University of Bedfordshire is a British University with four faculties, encompassing a number of schools, departments and divisions. In 2007, the University and 7Safe created a joint MSc in Computer Security and Forensics.

Alan Phillips is Chief Executive Officer and co-founder of 7Safe Limited. A Member of the British Computer Society, he has a background in computer security and holds a Business degree from Edith Cowan University.

7Safe is a leading Information Security and Computer Forensics company offering consultancy and education services across a wide range of disciplines within digital security and forensics including intrusion forensics, penetration testing, PCI DSS compliance and e-discovery.

The company is co-author and publisher of the 'ACPO Good Practice Guide for Computer-Based Electronic Evidence' (2007) available online at http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

The 7Safe forensic incident response / data compromise investigation team is experienced in both the Hi-Tech law enforcement and commercial arenas, conducting breach investigations for a vast array of clients including major retailers/department stores, Government agencies and acquiring banks.

The compromise investigation team led by Managing Consultant Benn Morris consists of an array of skilled technical consultants with diverse technical backgrounds. The team has analysed hundreds of computer devices in many different environments and scenarios, gathering a wealth of interesting data on which this report is based.

All data in this study is based on genuine completed breach investigations conducted by the compromise investigation team over the last 18 months.

University of Bedfordshire

7safe®

## Acknowledgements

S. Bhala
M. Christodoulides
L. Cornwell
R. Jones
B. Morris

Preface i

Introduction 1

Results and Analysis

Study Data 5

Number of Employees 9

Types of Data Stolen 10

Source of Breaches 12

Attack Sophistication 19

Attack Origin 20

PCI DSS Compliance 21

Conclusions 28

References 29

# Introduction

The way businesses operate has changed drastically with time. Continually striving for leaner, more efficient and timely services, they have embraced a number of innovations in process and technology. From refining processes in industry, to automation, to service delivery, businesses strive for ways to maximise revenue and minimise cost.

In more recent times however there has been an increased focus on customer service. Providing tailored solutions at a cost effective price has become the mantra rather than one-size fits all ethos of the early and mid twentieth century. As such, we are clearly in an era where information is the key for businesses to thrive; never before has information been so important. However, with the digitisation of so much information, so comes the ease of transmission and also theft, loss and leakage. In a recent survey 84% of organisations surveyed suffered at least one data breach in a 12 month period between 2007 and 2008; 44% suffered between 2 and 5 breaches [8].

The proliferation of electronic systems and ubiquity of access to the information they hold has given rise to increased opportunity for the criminally minded. A term of science fiction films twenty years ago, cybercrime is now a very real threat facing businesses.

There are a number of definitions for the term cybercrime and these typically differ in their acknowledgement of the breadth of crime that can be included under the term cybercrime.

The European Committee on Crime Problems of the Council of Europe [12], building on earlier work of the OECD [13], produced a set of guidelines that listed activities that should be considered criminal acts. The committee stopped short of a formal definition, opting rather to discuss activities that should be considered and thus allowing individual countries to adapt the functional classification to formulate tailored legislation in keeping with their own experience, preference and existing legal system. Others widen the definition to include such acts as fraud and child pornography. The United Nations Manual on the Prevention and Control of Computer Related Crime [14] states that cybercrime “can involve criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are generally subject everywhere to criminal sanctions.”

We present a definition for cybercrime that is based upon experience and the work discussed in the paragraph above. We recognise that this definition may differ from others and do not claim this to be more exact than any other. Rather, in keeping with the observation of the UN [14] which states definitions “have been produced [that] tend to relate to the study for which they were written”, we present a definition that is pertinent to this work, and anticipated future work. It is for this reason we choose a very loose all-encompassing definition.

# Defining Cybercrime

An act of cybercrime is any act which relies significantly or entirely on the use of one or more computers and gives rise to a result that is, or has a traditional counterpart that would be, subject to criminal sanction.

The above definition therefore covers all legislated computer crime, as well as cases in which computers are used in a significant manner, to commit any crime.

In its early history cybercrime was largely perceived as being undertaken by covert small groups or individuals driven by a sense of boredom or academic curiosity. Some of the earliest known hackers were the 414s, a group that gained notoriety in the early 1980s by breaking into high-profile computer systems. When eventually caught, the group's spokesman announced that the motivation behind what they had done was purely the challenge.

Times have changed however, and there has been a growth in cybercrime for a variety of reasons ranging from vandalism, through peer-group respect to political motivation. The most significant rise, and largest reason for the activity today, however, is for financial gain. As such, companies in sectors that rely on data that can be easily used for financial gain are particularly susceptible. We must acknowledge that while it is obvious that cybercrime is increasing year on year, the actual reported figures in any year are unlikely to be accurate. The 2009 UK Cybercrime report by Garlik [15] states very early in its proceedings that "official statistics will not reflect the true volume of cybercrime being committed".

Given the massive rate of adoption of electronic and web-based information systems, it is unsurprising that there is an ever-increasing occurrence of illegal electronic action. However it should be noted that it is not only credit card data that is of financial significance to companies and potential attackers. Intellectual property is often digitised and can have huge value. There has been a rise in electronic espionage and the threat is now affecting more companies than it did previously. E-espionage can be defined as "unauthorised and usually criminal access to confidential systems or information for the purposes of gaining commercial or political advantage" [16]. MI5 states that intelligence services "are targeting commercial enterprises far more than in the past." (http://www.mi5.gov.uk/output/espionage.html)

One of the greatest targets for attackers (particularly opportunistic hackers) is that of payment card data. The value of records of payment card data may have fallen, but the search for such records has not diminished. If it is a relatively easy task to acquire 500,000 credit card records (not at all an unusual number to be held on a system) then a business case for a criminal may well hold.

A crime closely associated with the theft and fraudulent use of payment card details, identity theft, is a significant problem that does not seem to be abating. It would appear that criminals are developing their skills and techniques more rapidly than security engineers and enforcement officers.

# About this Report

There has been a great deal of interest in data security breaches in recent years and this interest has led to a large number of surveys, most notably the series of nine DTI Information Security Breaches Surveys (the most recent report being published in 2008 [5].

Whilst the information garnered from such reports is very useful, and indeed can be used to form a business case for information security budget increases, the problems with such surveys are well documented. The foremost important problem is that at best there is lack of confidence in the accuracy, if indeed the data is accurate.

The aim of this report is not to comment on a recent study, but actual forensic analysis of data breaches. This work analyses 62 genuine cases of breaches investigated over a period of 18 months. These investigations have been conducted by the digital forensics team at 7Safe. The breaches vary in many ways, including the sector they belong to, the number of records at risk and the sophistication of the attack. This report presents statistics on the investigations and discusses the data to provide a greater understanding of underlying trends.

For any crime we would like to know the "who, where, when, what, how." In terms of ensuring that justice is served to the person responsible for a crime, the "who" is obviously critical. However, finding out who committed a crime is more important than just to ensure they receive the appropriate punishment as a penalty for the crime or to satisfy a victim in some form of revenge. By demonstrating the ability to determine who perpetrated an attack and then punishing appropriately, we can deter future potential attackers from committing a crime.

Determining where a crime was committed is useful even in electronic crime situations. Information on the geographical location of the origin of a cybercrime can assist in determining the laws to which that individual should be subject to. It can also provide information to help ensure that the number of future attacks can be reduced, or that the effect of future attacks is diminished, by undertaking appropriate preventative action.

Working out when a crime was committed is important for a number of reasons, not least of all because it can both assist in the identification of the attacker, but also without this information it is very difficult to successfully prosecute a criminal. It is also important because knowing the time of the attack can allow investigators to determine the state of the system at the time. It may be that since the initial breach was started the system has been patched and is now not vulnerable to that attack.

Ascertaining what has been compromised is a non-trivial matter, as the business of analysing cybercrime can prove to be a difficult undertaking. The Garlik UK Cybercrime Report [15] states "quantifying cybercrime is an imprecise activity". A recent report on E-espionage also comments that the "lack of specific management information about the number, nature and source of breaches is a worrying finding." [16]

The problem has even been made aware to the Government and the House of Lords Science and Technology Committee recently commented:

> *"The availability of comprehensive and reliable data about e-crime - the scale of the problem, the risks to the public and the costs to the economy - is fundamental to developing an effective response to the problem*

*of e-crime and to promoting public confidence in the Internet. We urge the Government to implement proposals in response to our recommendation on data collection and data classification without further delay." [17]*

One of the important roles of a forensic investigator is to determine how a compromise was achieved. This is pivotal to the containment of the problem, and will also help identify the data that has been compromised. Analysis of how a breach occurred will allow information security strategists to decide how to prevent further breaches occurring through the same vulnerability.

It is important to reiterate that any statistics for cybercrime are fallible and will only provide details of that particular sample. There can be no assumption that the statistics can necessarily be extrapolated to make a judgement about a national or international landscape. The statistics presented are based on the 62 reported cases undertaken by the 7Safe forensic investigation team. The value of the information will vary from reader to reader, but we believe there are a number of insightful details that have been brought to light through the report.

It is imperative to understand the importance and value 7Safe holds for its clients and the protection of their data. 7Safe is committed to maintaining both the privacy and the anonymity of its clients. As such, all data used for analysis was sanitised and client names removed from records. The data contains no information that would allow the client's identity to be derived. Equally, the method of presentation of statistics within this report is in such a way so as to ensure that it cannot be individualised to gain information about any client; the data presented is always in an aggregate format.

# The Study Data

The data used in this study is taken from genuine, sanitised information taken from real investigations by the forensic analysis team at 7Safe. The data covers companies from a range of business sectors including the financial, sport and retail sectors. Data security breaches can be seen to affect organisations across a wide range and no particular industry that utilises electronic systems can claim to be exempt from threat.

It has, of course, been recognised that the risk a company faces is dependent upon a number of factors. In particular, the sector in which an organisation operates is known, and for obvious reasons to impact upon both the level of threat it faces and the nature of the attack vector. On 19th March 2008, the British Prime Minister Gordon Brown presented the Government's new National Security Strategy to the House of Commons. This was followed in August 2008 by the National Risk Register, a component of this strategy released by the Cabinet Office. It provides an official Government assessment of significant potential risks to the United Kingdom and divides risks into three main categories: natural events, major accidents and malicious attacks. It evaluates risks and rates them by relative impact and relative likelihood. The National Risk Register states that "The risk and impact of electronic attacks on IT and communication systems varies greatly according to the particular sectors affected and the source of the threat." [18].

The sector details of the cases investigated by 7Safe and featured in this study can be seen in figure 1.

Figure 1 shows quite clearly the dominance of the retail sector in this study, which is not uncommon to other studies and surveys concerning data breaches. This is not surprising and is likely to be a feature of all studies concerning non-sector specific breach investigations, though perhaps the proportion of those in the retail sector may not be quite as high as in this particular study in which the vast majority of the attacks were on organisations in the retail sector.

The retail sector often keeps data regarding a large number of credit card transactions that can then be used for cardholder not present (CNP) transactions. It is therefore one of the major reasons that the sector is targeted for financial gain.

The Association for Payment Clearing Services, APACS, was the trade organisation for the co-operative activity of banks, building societies and card issuers on payments and payment systems and was established in the mid 1980s. APACS ceased to exist on 6 July 2009 but has been replaced by the UK Cards Association. A report by APACS [19] detailed that CNP fraud was valued at £328.4 million in 2008; this was a rise of 13% on the previous 12 months. CNP fraud involves the theft of genuine card details that are then used to make a purchase over the Internet, by telephone, or by mail order. The cardholder is usually unaware of this fraud until they check their statement and this gives the criminal opportunity to receive goods or services and use them or sell them on before the crime is even detected. CNP is the largest type of card fraud in the UK and accounts for more than half of all card fraud losses.

It should be noted that while CNP fraud has risen over time, so too have the shopping habits of consumers, and as such the year on year increase should not be a surprise. From 2000 to 2008 CNP fraud rose by 350 per cent; however over the same period, the total value of online shopping increased by 1077 per cent. In 2008 online shopping accounted for £41.2 billion compared to the much more modest £3.5 billion in 2000.

Whilst it can be reasoned as to why there may be such a large number of investigations regarding the retail sector, the statistic should be viewed with some caution. The number of organisations in the retail sector is a significant proportion of UK organisations and as such, it would be expected to feature highly in any report on investigations. It should also be noted that losses from a large number of retail organisations may not necessarily be as high in value as a single loss from a company in the financial sector nor indeed from a manufacturing company which has lost intellectual property of significant value. Furthermore, it has been suggested that there has been an increase in the number of investigations of breaches suffered by organisations in the financial sector. This may represent an actual increase in the number of breaches, but it is important to note, that a substantial number of breaches may have been experienced for some time, but the investigation of these breaches kept internal.

Companies in the financial sector are often particularly susceptible to volatile share prices that are elastic to confidence in the services they offer. As such, they prefer to keep details of, or indeed existence of, breaches out of public awareness and employ internal teams. A recent research paper has summarised the situation quite well:

“The absence of a breach notification is not the same as the absence of a breach. An undetected breach cannot be reported. A compromise that is detected internally may not be communicated to the larger public, either because the likelihood of a threat having exploited a vulnerability is deemed too unlikely, or because the organization determines that it would rather accept the consequences of a lack of disclosure than the additional expenditure that might result from publicizing a compromise. Though breach notices provide imperfect information” [20]

It may be that these organisations are now outsourcing more of these investigations which would lead to a rise in the number of investigations undertaken by external agencies. It should be noted that it is also likely that the number of attacks against those in the financial sector is likely to have risen itself, and in the data used for this study, the second-most investigated sector was financial. It has been reported publicly that some financial organisations were victims to sophisticated attacks in 2008.

Beyond the retail and financial sectors, there were a wide number of different sectors that were investigated after breaches including councils, health, hospitality, IT services, marketing, metal trade, postal and sports; some of the organisations investigated had multiple businesses across different sectors.

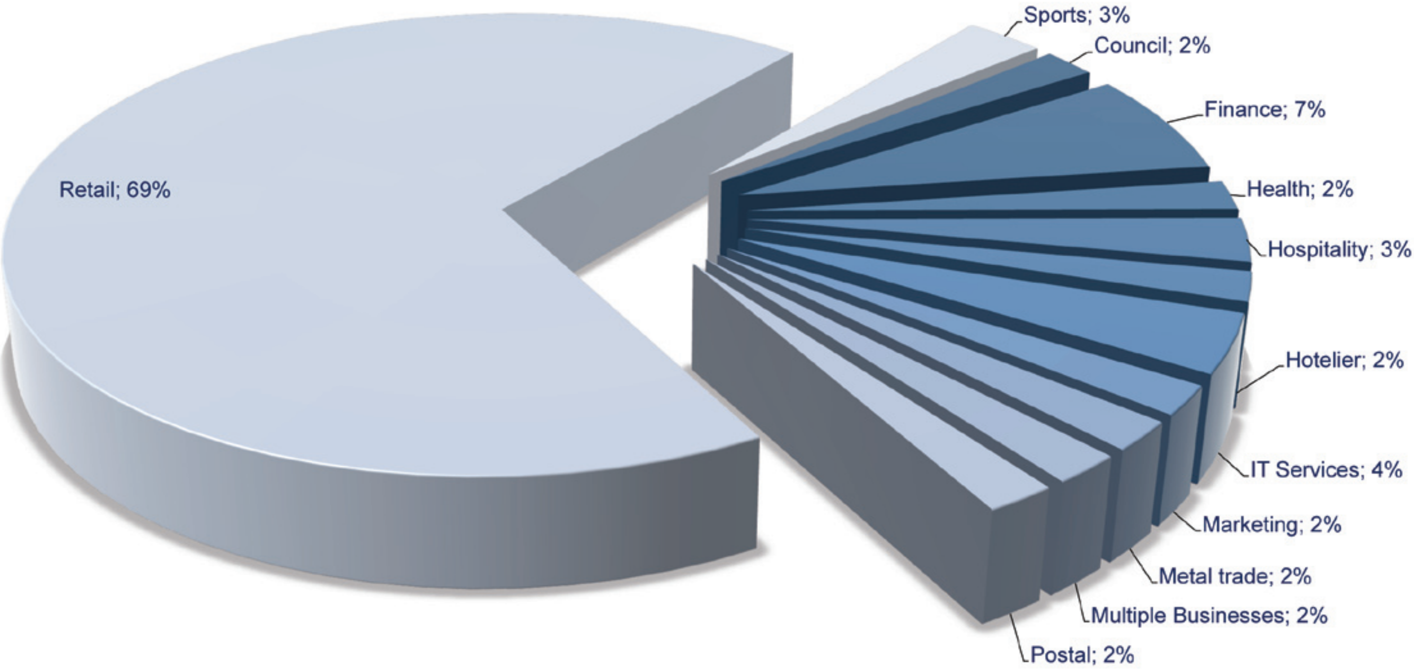
The organisations for which data has been gathered for this report can also be categorised using Standard Industrial Classification (SIC) codes. The SIC system is used for classifying business activities in the UK and is bound, by European legislation, to the European Union’s industrial classification system, NACE (Nomenclature Générale des Activités Économiques dans les Communautés Européennes). The SIC and NACE codes systems are most widely used for statistical analysis by authorities and statistical bodies. There have been three different versions of SIC codes, the first in 1992 which were revised in 2003 before forming the basis for the UK 2007 SIC system. The changes have largely been due to refinements due to changes in services offered in the area of technology, particularly information and communications technology.

The development of the system has involved a number of stakeholders such as the European Commission, the National Statistical Institutes of EU member states, European Business and Trade associations, the Bank of England as well as a number of UK Government departments.

The organisations that have been investigated are presented by the SIC codes in Table 1. This demonstrates the wide range of primary SIC codes for the organisations of this study.

FIGURE 1

ORGANISATION BY INDUSTRY TYPE



*Type of oganisation based on industry type.*

TABLE 1

STANDARD INDUSTRIAL CLASSIFICATION CODES

| SIC CODES 2007 | SIC Code Classification Name | Number of Occurrences |
|---|---|---|
| 47910 | Internet retail sales (retail) | 41 |
| 66190 | Financial transactions centre | 3 |
| 62012 | Business and domestic software development | 1 |
| 96040 | Spas | 1 |
| 62020 | Information technology consultancy activities | 1 |
| 16230 | Fencing made of wood (assembled) (manufacture) | 1 |
| 64929 | Finance corporation for industry | 1 |
| 24420 | Aluminium alloys production (manufacture) | 1 |
| 62012 | Web page design | 1 |
| 63110 | Web hosting | 1 |
| 73200 | Market research agency | 1 |
| 93120 | Football clubs | 1 |
| 84110 | Local Government administration | 1 |
| 55201 | Holiday and other short stay accommodation, provided in holiday centres and holiday villages | 1 |
| 65120 | Motor insurance | 1 |
| 82990 | Luncheon voucher company | 1 |
| 55100 | Hotel (licensed with restaurant) | 1 |
| 24100 | Engineering steel (manufacture) | 1 |
| 77110 | Car hire (self drive) | 1 |
| 93199 | Rugby league | 1 |

***Organisation industry type by SIC classification.***

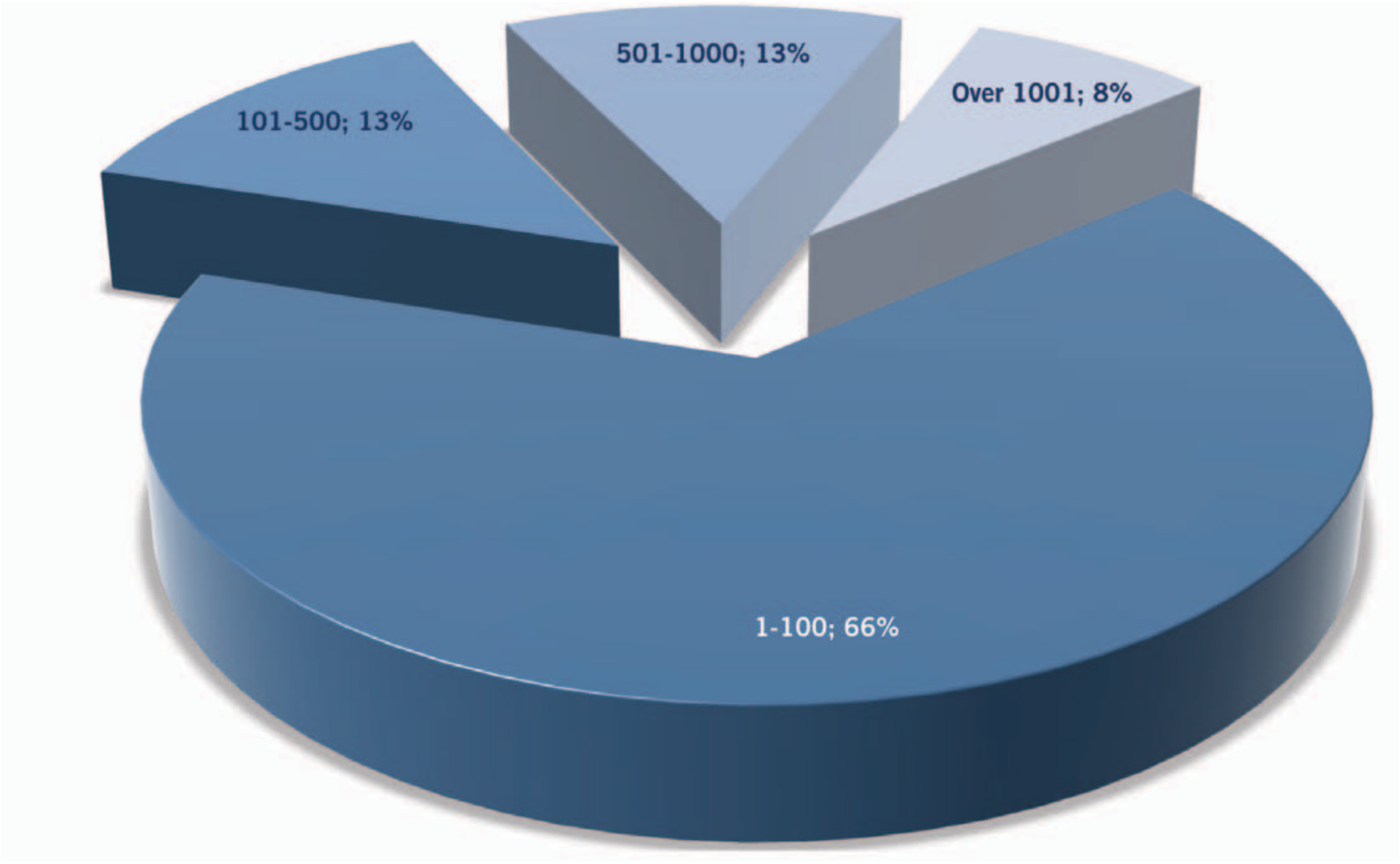
## Number of Employees in the Organisation

The organisations used to comprise this report vary widely in size. The vast majority of organisations that were investigated had between 1-100 employees. It has been widely reported that as the motives of attackers has moved from vandalism to financial gain, so too has the target of those attacks.

Many of the attacks primarily aimed at vandalism would have been at the largest companies, so as to cause maximum disruption, but when attacking for financial gain the strategy changes. Attackers will now consider a simple return on investment argument along with an appropriate risk analysis. With larger companies investing more in security and incident response, the great returns from an attack require more effort and carry a greater risk than undertaking multiple attacks against smaller companies.

FIGURE 2

NUMBER OF EMPLOYEES IN THE ORGANISATION



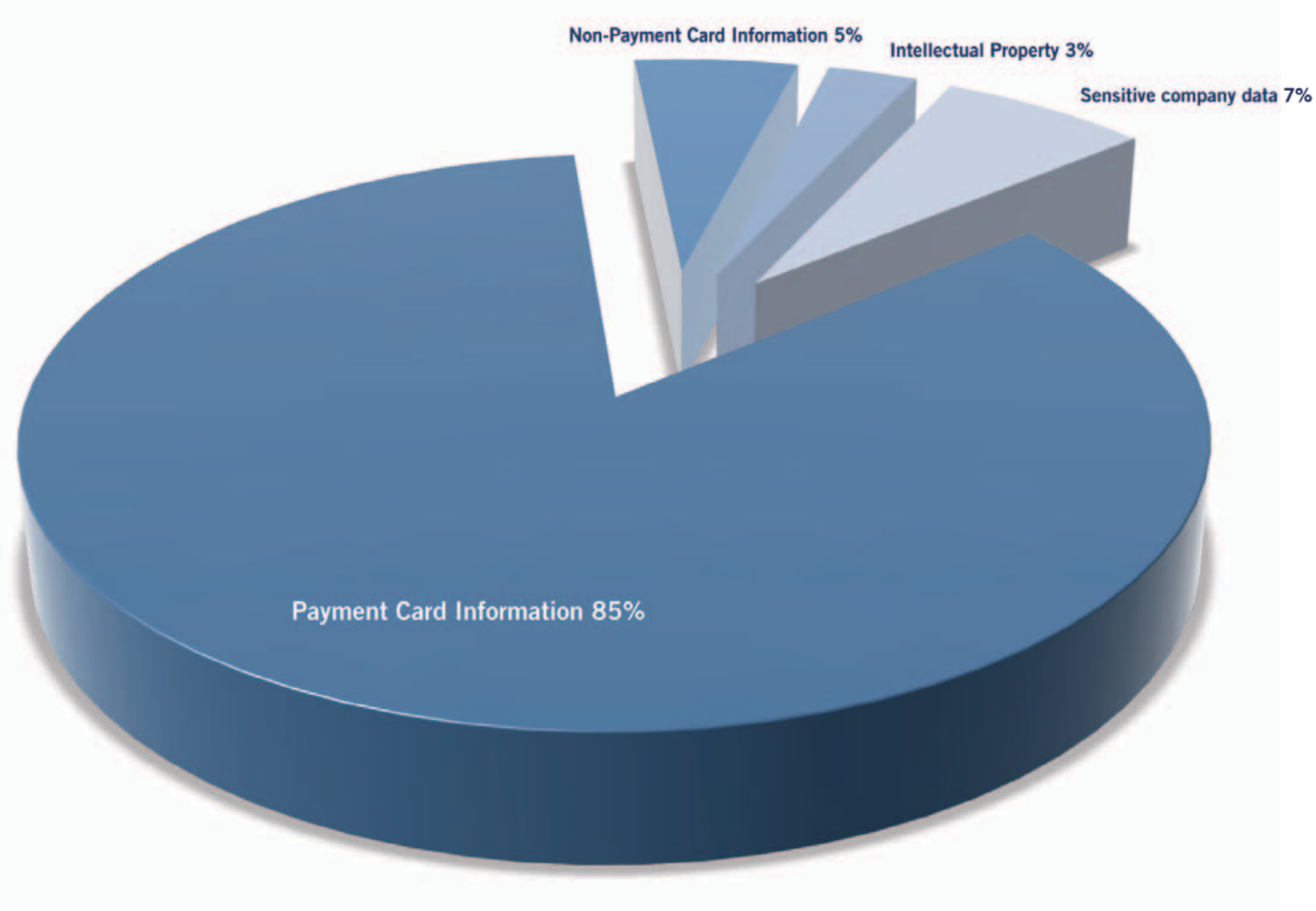
*Number of employees in the organisations investigated.*

# Types of Data Stolen

As has been mentioned it is important, but often difficult, to ascertain exactly what data has been compromised. In the cases investigated the vast majority involved payment card data being lost or leaked; payment card data was compromised in 85% of the cases. This can be attributed to the fact that the data is in a readily available and useable form. It can lead to financial gain with very little effort and this is of great attraction to cybercriminals looking for a rapid return on their effort.

FIGURE 3

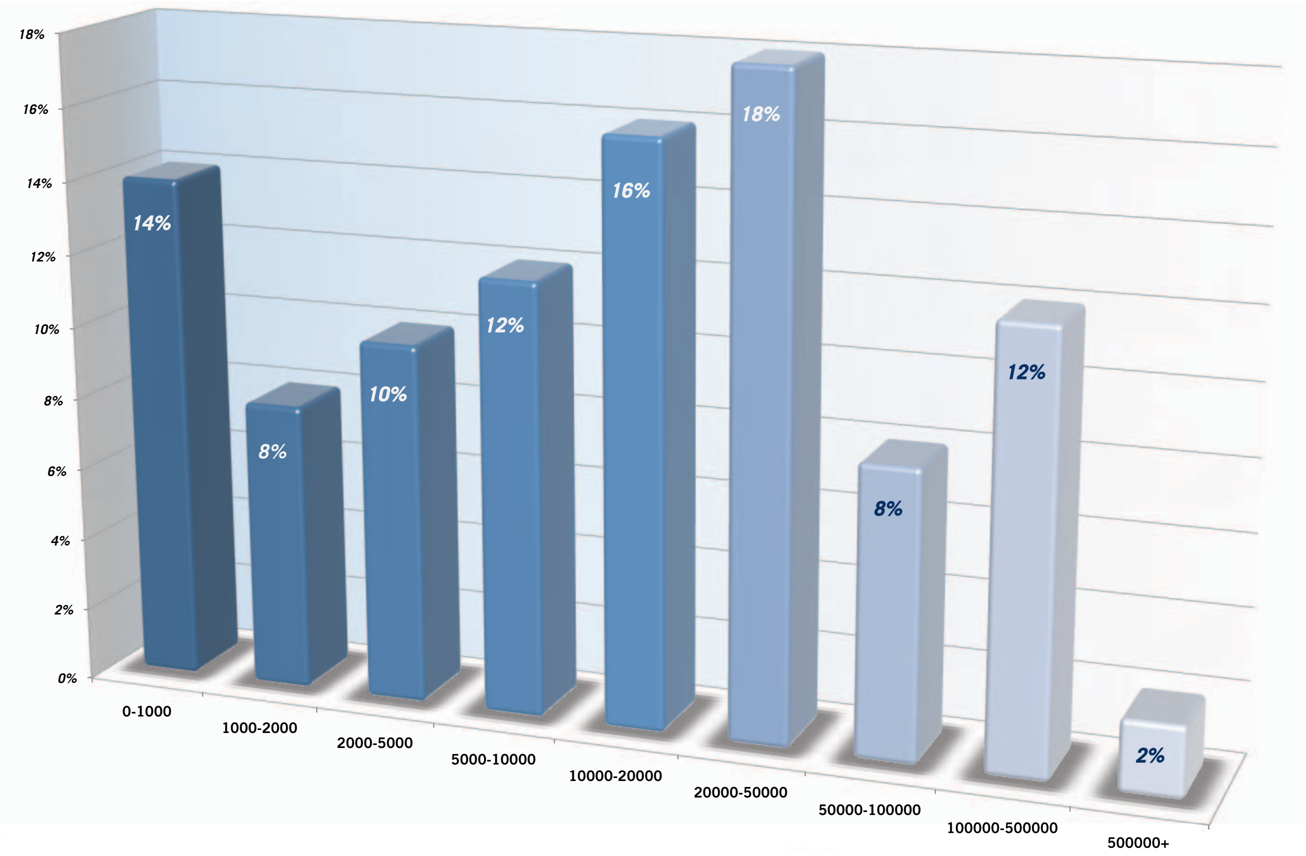
TYPES OF DATA STOLEN



*Types of data stolen from the organisations investigated.*

FIGURE 4

NUMBER OF CARDS AT RISK



***Cardholder records at risk.***

Where payment cards were at risk, the range of card numbers involved varied, with the most common being between 20,000 and 50,000, across all investigations.

# The Source of Breaches

As with any crime there are a number of questions to be answered. One of the important questions is who committed the crime. This is needed for a number of reasons, but most notably to ensure that justice is served. Unfortunately this is not always possible, and is often the case in electronic crimes. Criminals can use techniques to cover their tracks, spoof their identities and their locations.

It is a well-known problem in information security and forensic analysis that even when a particular piece of equipment can be tracked with absolute certainty to be the source of a crime, proving the specific perpetrator is non-trivial. This is even the case when the machine can be proved to belong to an individual, or a password is used, or even after an analysis of other interactions with the machine is performed. However, it is the role of the forensic investigator to ascertain as much information regarding the identity of the perpetrator as possible, and potentially give evidence in court to help determine beyond reasonable doubt whether the accused is responsible.

An early fact that investigators consider is where the attack originated in relation to the organisational structure. That is, to establish whether the attack was internal, external or through a business partner. This can also be used to identify trends and which threats are actually realised. It is such information that can inform the assessment of the risk and associated loss as well as the strategy for recovery and prevention of further breaches through similar attacks.

It should be noted that the source of an attack is recognised to be closely correlated with industry, and this may be for a variety of reasons. For example, all attacks on financial organisations were from external sources; this could be explained by recruitment policies or regulation within that sector.

Internal sources are those that originate from within the organisation itself. This would typically be the staff in the organisation and is not restricted simply to those in an IT department but all staff from the board through end users of IT systems to cleaners and maintenance staff, and indeed the work experience student in the office for only a few weeks. It should be noted that as well as the staffing aspect of an organisation, internal sources will include physical assets such as paper based information that can be used to assist in a breach or information systems on the premises that are open. Insider threats can be particularly devastating as all insiders will have some level of privilege and trust, and some insiders have very high levels of both.

External sources are those that originate outside the organisation and are attributable to a person or group of people that have no relationship with the organisation. These are often in the categories of hackers, organised crime groups, and Government entities. Being external to the organisation, the levels of both privilege and trust will be minimal in most cases (though unfortunately this may not be true in certain cases.)

Business Partners are any people or groups that have a business relationship with the company. These third parties may be in the same, vertical or horizontal sectors to the organisation and will include, but not be limited to, suppliers, customers and contractors. Since most business partners are chosen and in some way controlled, they and their associated staff do enjoy some level of trust and privilege. However, since the recruitment and development of staff is not directly controlled (nor indeed might the contractors chosen by a business partner be approved) the level of privilege and trust is generally lower than that of an internal member of staff.

A weakness in the business partner scenario is that if an attacker compromises the partner and then uses trusted connections to access the victim, it will appear to the victim that the attacker is actually the trusted business partner and as such will have access to all the data that would be available to that partner.

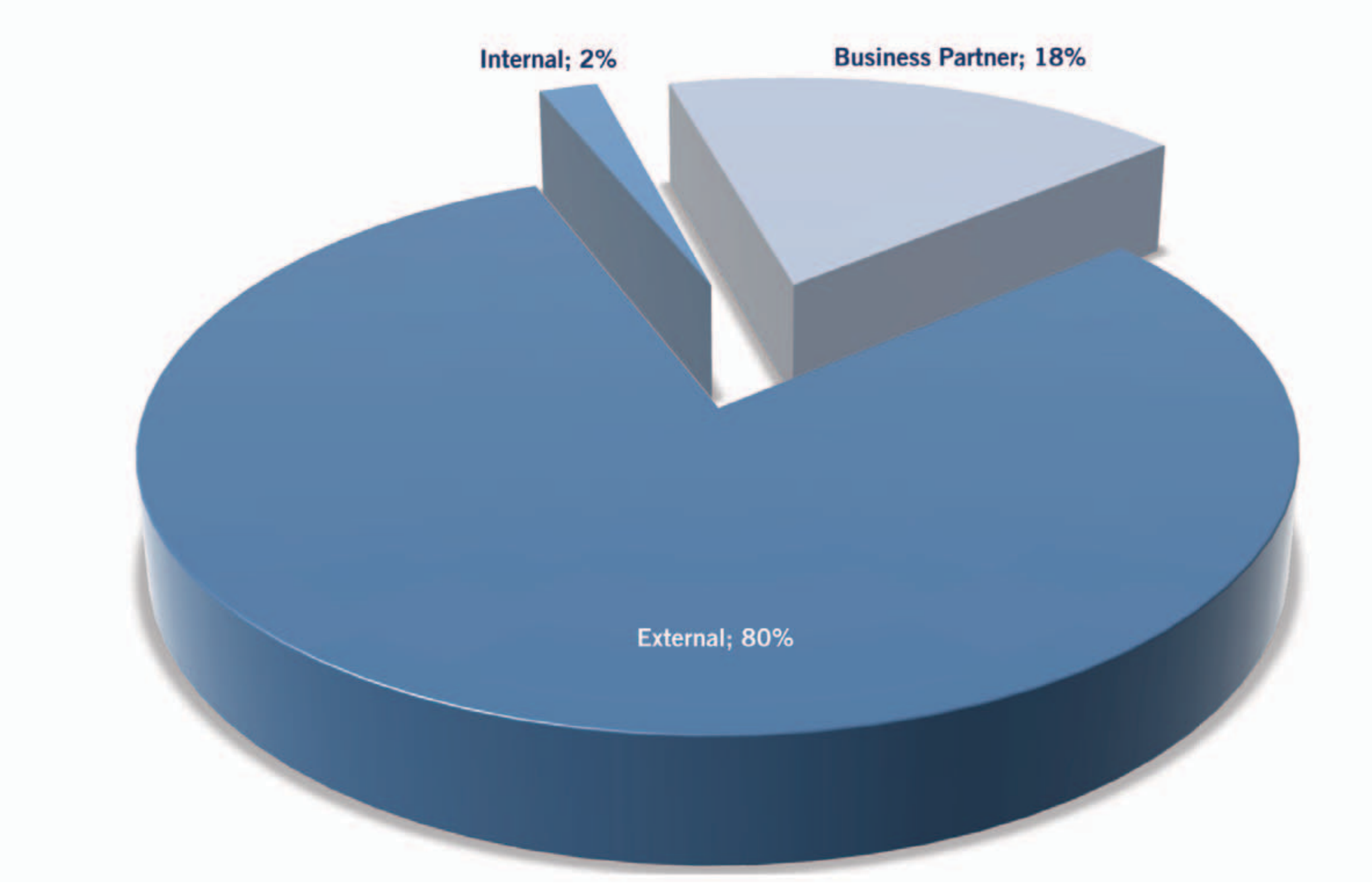
The forensic investigators at 7Safe have determined what the primary source of a breach is. A source is considered a primary source of a breach if it was the most significant reason behind an attack.

As can be seen the majority of attacks in this study were from external sources. Indeed the number of attacks that were down to internal sources is a very small minority. This may seem counterintuitive to some observers, and indeed may contradict some survey data in other reports. For example the third edition of the Global Security Survey for the Technology, Media & Telecommunications (TMT) industry, found that 41% of respondents experienced at least one internal security breach in the 12 months leading up to the survey. Indeed only 28% of respondents rated themselves as "very confident" or "extremely confident" with regard to internal threats, down from 51% in their 2008 survey. [21]

It is not claimed and should not be assumed that the actual proportion of breaches that are due to internal sources is consistently this small; we can only report on the cases undertaken by the 7Safe forensic investigation team.

FIGURE 5

SOURCE OF BREACH



The data analysis shows that 18% of breaches were primarily due to business partners. This highlights a concern that is often left from consideration but is of importance. It is critical that companies recognise the lack of control they have over business partners. They need to be aware that some of the arrangements their partners have with other external organisations may allow full access to all information held by the partner, and by transition therefore have access to information of the original company. This has been seen in more than one case that 7Safe has investigated.

Given the sheer volume of attacks that originate from hackers, it is important for forensic analysts to determine the techniques employed. Using this information is of great benefit to information security officers that can then ensure hardening of the systems against future attacks. The cases examined by the 7Safe forensic investigation team show the predominant vulnerabilities exploited were in poorly written website applications, and in particular, by SQL injection and malware attacks.

In the study 40% of all attacks utilised SQL injection as the source of the compromise with an additional 20% on top using SQL injection combined with another vulnerability such as malware (see figure 8). The SQL injection vulnerability is a common weakness in many systems as can be seen with 60% of the cases suffering from it leading to the compromise. However, it is surprising given the amount of information known about the attack and ways to prevent it that so many systems are still susceptible to it. SQL injection attacks take advantage of poor coding practice in applications and web interfaces by exploiting a failure to properly handle user input. It could be argued that in complex applications and live systems it can be difficult and costly to repair all flaws that result from failure to validate SQL input. However, this must be the responsibility of the information security analysts, and they are only equipped with finite resources and a growing numbers of potential threats. The fact that many compromises come from SQL injection attacks can only help inform the decisions that an information security strategist makes. This heightened risk can be used in a risk assessment to produce a cost-benefit analysis. Estimating the cost for this analysis will rely on estimating the cost of repair to existing systems, and the extra protection afforded. This may become increasingly difficult as SQL injection attacks become more sophisticated. A large proportion of the breaches involved attacks on web interfaces and it is clear that this presents a major security risk for organisations.

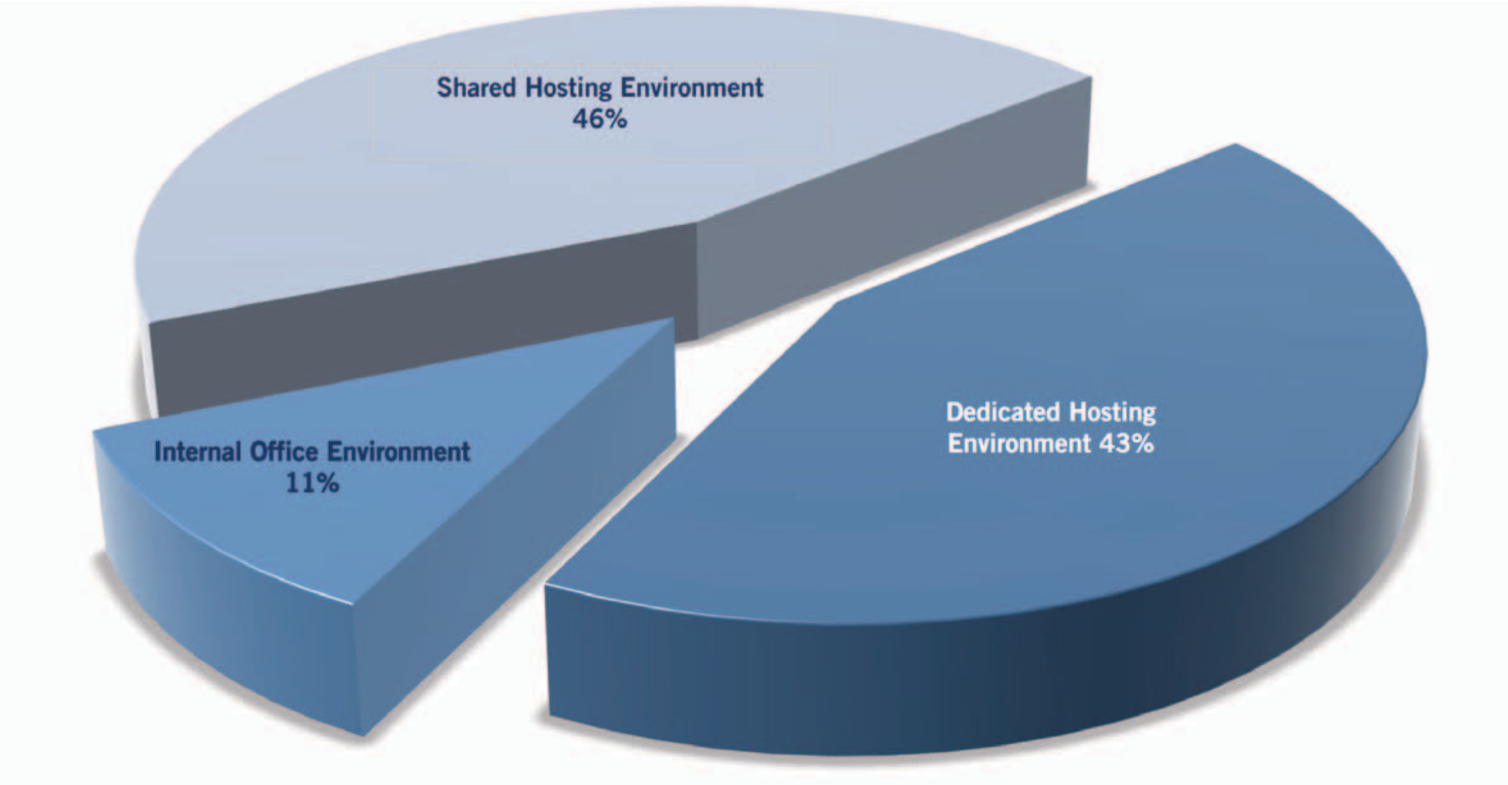
The benefits of allowing access to data via a web interface is clear, however the advantage must be weighed in the face of the risk. In some cases the advantages will outweigh the risk of data loss; in other cases it will not. It is for this reason that it is vital that access to data through the web for remote working must be customised and carefully planned. Access should be limited to those that specifically require it, and the information allowed should be strictly that necessary to allow effective remote working. SQL injection attacks are unlikely to be affected by such policies, but by considering access to data, it is possible to segregate data so that if a web server is compromised it is physically and logically separated from other corporate or customer information.

One of the ever-increasing sources of compromise is the exploitation through shared web space or web hosting. The dangers of shared hosting environments are as simple as an attacker compromising one website using malware or SQL injection, thus having the ability to compromise all websites on that hosting server using the same vulnerability. This is often seen in investigations carried out by 7Safe and the majority of the cases undertaken (46%) involve a shared hosting environment being hacked.

Malware continues to be an area of concern for those responsible for protecting information systems. Whereas historically the motivation for creating and distributing malware may have tended towards disruption or vandalism, financial gain is now clearly the main motivation. The average medium-sized organisation has been reported to experience five malware attacks per year and has seen threat levels increase each year.

FIGURE 6

ENVIRONMENT UNDER ATTACK



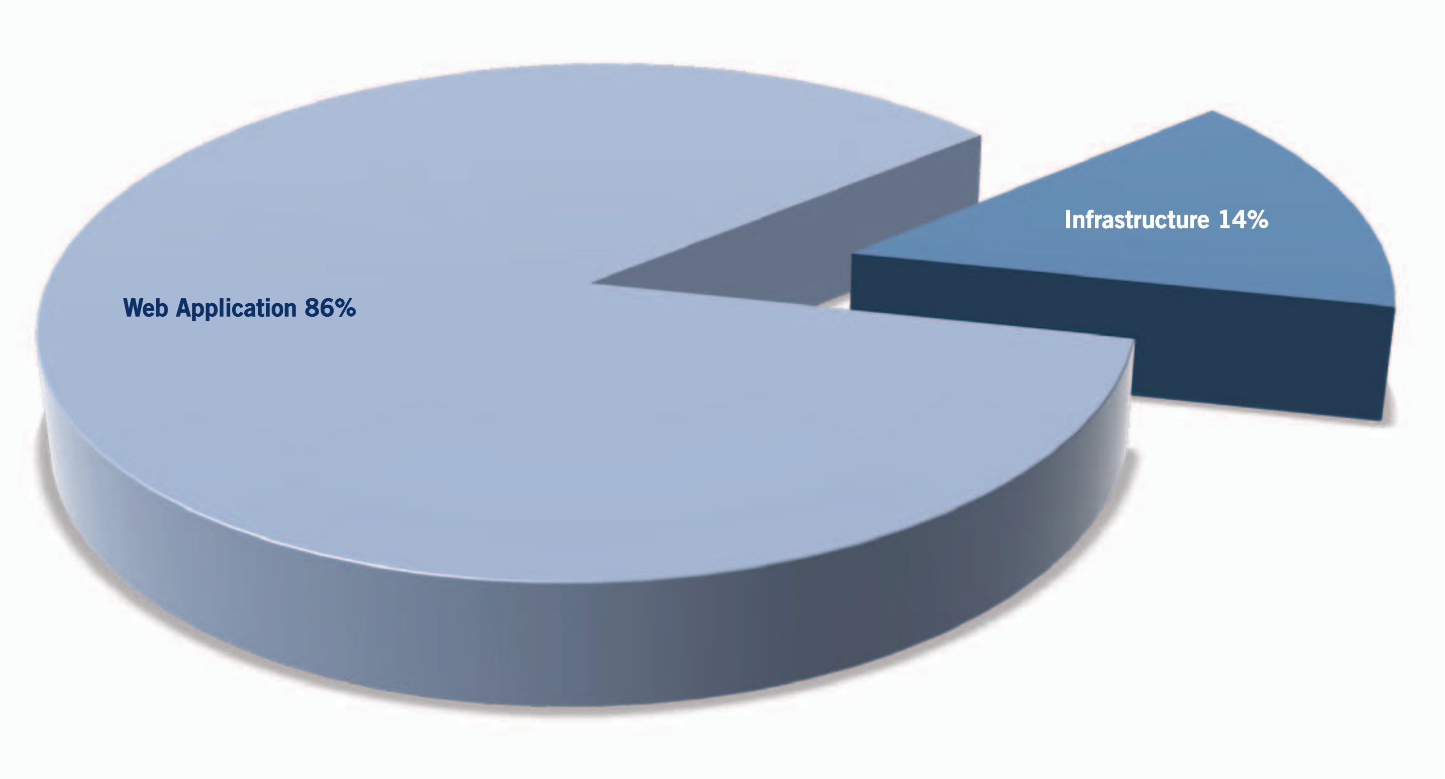
***The environment compromised that stored or processed the data at risk.***

## Infrastructure vs Application

Another interesting trend is the increased proportion of website applications being targeted for attack rather than the infrastructure it is hosted upon. The data used for this study shows that in 86% of all attacks, a weakness in a web interface was exploited. (see figure 7) . A likely reason for this is the inherent availability of websites versus that of its hosted infrastructure (including operating systems, hardware devices etc.). The reward of exploitation is often also more apparent. For example, an ecommerce website is clearly going to be processing cardholder data and be of a known higher value than a random IP address of a server on which the data may or may not be of any value to the attacker.

FIGURE 7

INFRASTRUCTURE VS APPLICATION



***Areas of the compromised systems exploited.***

## Exploited Vulnerabilities

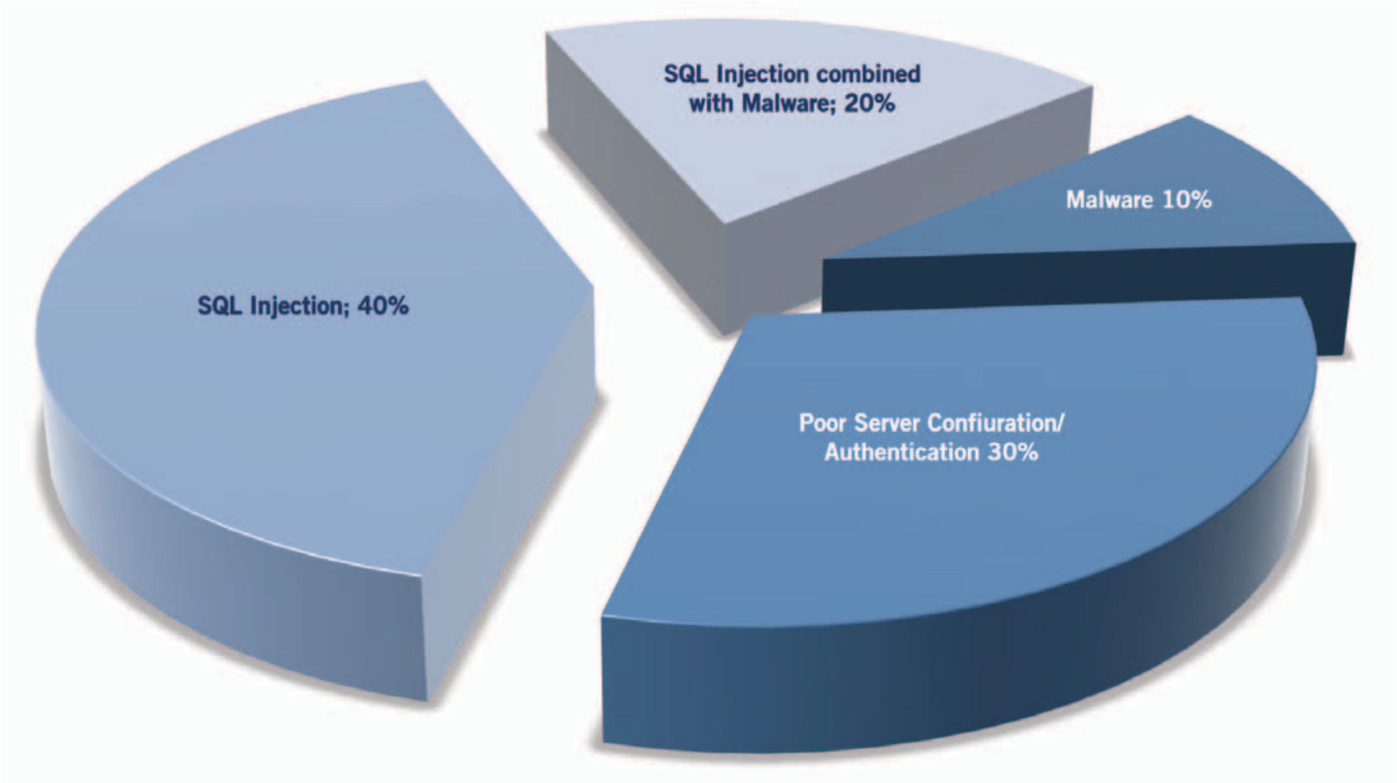
The most common cause of the compromises investigated are shown in figure 8. The main vulnerability exploited is SQL injection, with a notable increase in the rise in attacks using malicious software or malware being apparent over the course of the investigations during the study period. Commonly used malware in the form of 'web shells' has been seen in a high number of recent cases. This is most likely due to the simplicity of the infection into a website system. All the attacker requires is the ability to upload a file, be it from a Curriculum Vitae up-loader, an image uploader or a website authoring tool. The attacker doesn't even require the knowledge of how the web shell is written or how to code it, as it's simply a case of point and click. These web shells are often very well coded and quite complex in their functionality, but are freely available on the web and are ready to use on any vulnerable website.

Often SQL injection is used to facilitate the malware attacks. In recent cases investigated, SQL injection can be seen used to exploit and steal database usernames and passwords. The attackers then simply use these stolen credentials to access the administration interface of the website and use the built-in image upload facility to infect the site with the web shell, and start stealing data.

Poor server configuration describes a mis-configured server or one that has services running that has not been set up correctly. In the cases investigated there were many instances where administrator and user credentials were very weak or easily guessable; allowing an attacker to brute force the account to gain a foothold onto the system. In one instance, the attacker compromised a default known user account and logged onto the server using the remote desktop connection facility, and compromised the system. In this case the username was Guest and so was the password. The lack of protective equipment such as firewalls or hardware virtual private networks (VPNs) were also contributory factors to these types of attacks. Either they were not present or they were not configured correctly to prevent an attack.

FIGURE 8

VULNERABILITY LEADING TO DATA COMPROMISE



***Vulnerability or exploit used to compromise the system.***

## Attack Sophistication

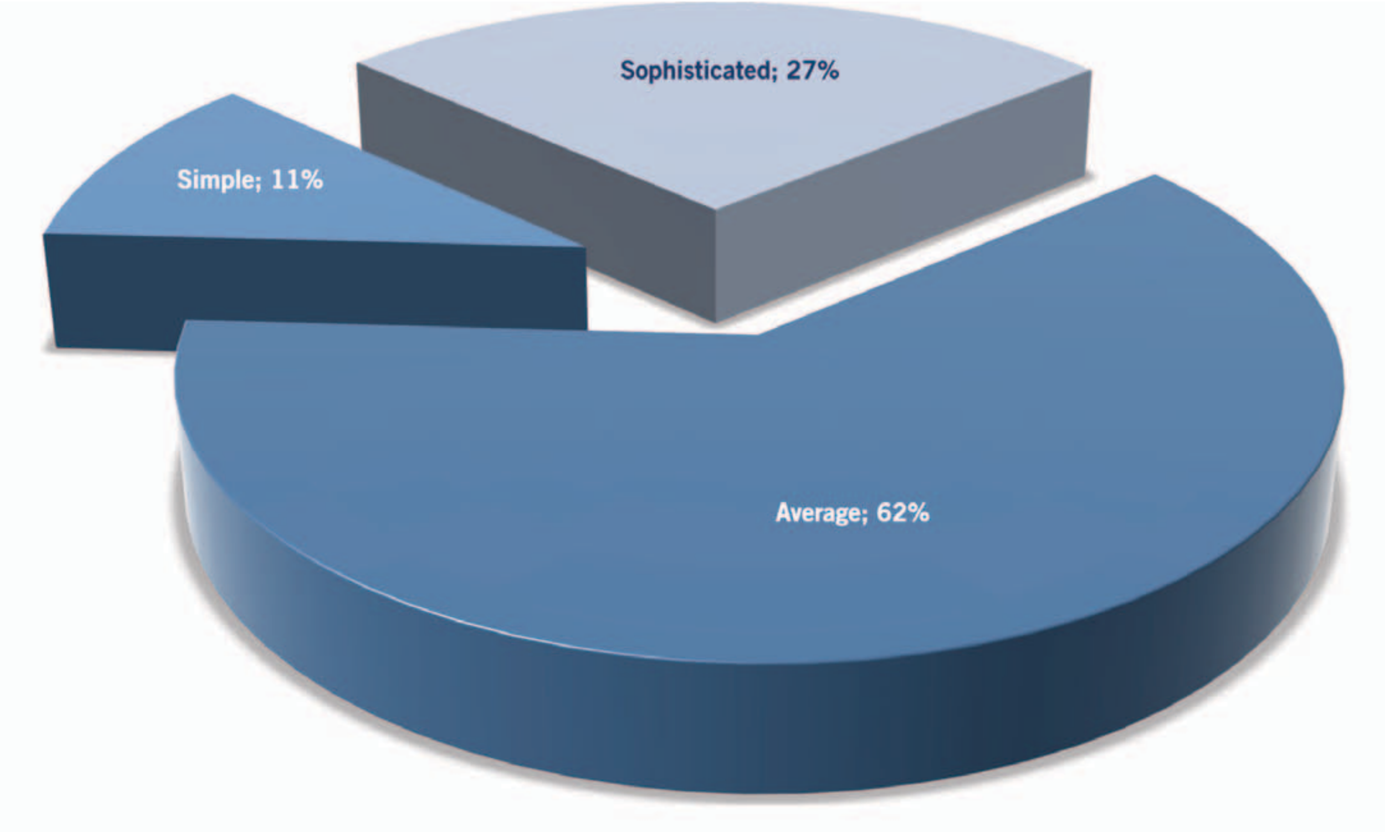
The sophistication of an attack is almost always a direct indicator of the difficulty of attack (since most attackers will choose the simplest way to break into a system). The difficulty of the attack can then, in turn, be considered an indication of the strength of the system under attack. The difficulty of the attack also demonstrates how much effort an attacker is prepared to go to in order to compromise the system in question. Classifying the level of sophistication is subjective and the experience of 7Safe forensic investigators has been used to classify the sophistication of the attacks. Simple: No specialist skills or resources are required to conduct a simple attack. Basic computer operation skills are required.

Average: This requires only basic tools without modification or knowledge. Many of the tools will be freely available from general Internet sites with high levels of automation. People using such tools are sometimes termed ‘script kiddies’.

Sophisticated: Advanced skills and knowledge, often in the areas of programming and operating systems, are required for sophisticated attacks. Such attacks normally require a level of preparatory work and involve a staged attack over a period of time.

FIGURE 9

COMPLEXITY OF ATTACK



***Complexity of the attacks investigated.***

## Attack Origin

Only 13% of the attacks on UK-based organisations appeared to come from the UK itself, with the majority emanating from the Vietnam and the US. The law in Vietnam during the study period was such that Vietnamese citizens could not be prosecuted for committing computer crime against foreign countries.

An important note when analysing these statistics is that they have assumed that the last IP address identified is the source IP address of the attacker. It is possible that the attacker could have compromised a computer in another country (or indeed a series in several locations) and used this as the final hop into the victim organisation.

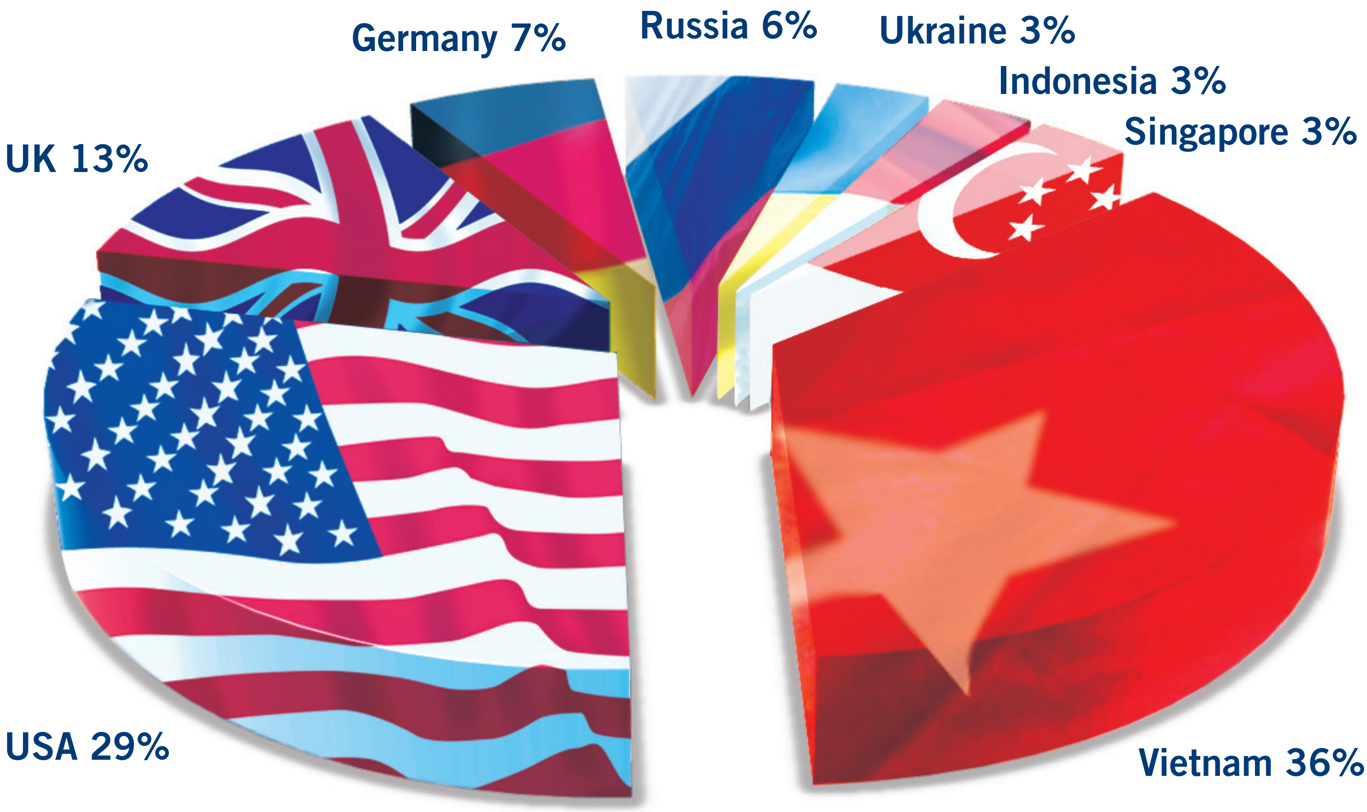
7Safe's forensic investigation team does not have the legal authority to investigate the apparent source of attack and beyond. However, on particular high profile cases, 7Safe has worked with the relevant law enforcement agencies to pursue these lines of enquiry.

Many of the attacks are conducted in such a way that there is no trace of the attacker's IP address stored on the server and therefore their potential location is unknown. Also a large number of investigations have been conducted on servers on which log files were not present, not configured to be stored, or corrupted. Many system administrators and web designers do not see the value in enabling logging on their servers due to the potential high amount of disk space required.

However, it is also apparent that some hosting companies also limit the amount of log files stored by default, e.g. for one week. Therefore, this highlights the need to act fast in engaging a forensic Incident Response team such as 7Safe's in order to preserve the best evidence for the investigation.

FIGURE 10

ATTACK COUNTRY OF ORIGIN



# PCI DSS Compliance

There are a number of data security standards to which organisations should comply with, depending on the circumstances in which they operate. These include Sarbanes-Oxley Act of 2002 (often referred to as SOX), Basel II, Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA).

One of the most important is that developed by the Payment Card Industry Security Standards Council (PCI SSC), "an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection." (https://www.pcisecuritystandards.org)

Founded on 15 December 2004, the mission of the PCI SSC is to enhance payment account data security through education and awareness of the Payment Card Industry Data Security Standards (PCI DSS). American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc founded the PCI SSC.

Organisations that store, process or transmit cardholder data and fail to comply with the PCI DSS face the risk of not being allowed to handle cardholder data and fines if the data is lost or stolen.

A large number of the breach investigations undertaken by 7Safe included the compromise of cardholder data, which encompasses credit and debit card numbers ('primary account numbers'), card security codes and other account information such as cardholder name, expiration date etc.

There are twelve requirements of the PCI DSS within six categories. The requirements each contribute in different ways to ensuring the protection of data and the subsequent impact of any breach. Upon investigations where cardholder data was compromised, the 7Safe team checked compliance with each requirement of the PCI DSS.

These categories and requirements are presented below, along with the results of the analysis.

## Build and Maintain a Secure Network

### *Requirement 1: Install and maintain a firewall configuration to protect cardholder data*

Requirement 1 is defined to ensure that access to and from a network is authorised. Firewalls can be software programs, hardware devices, or combinations of both and are generally used to monitor the information coming through an Internet connection into a computer system.

It is vital that only authorised access is given to the cardholder data environment. This issue however does not only relate to Internet connections but must also consider segmenting access from other untrusted networks, including wireless networks.

Whilst many of the organisations investigated actually had firewalls installed, poor configuration of these devices rendered most of them useless. In over 96% of cases, requirement 1 of PCI DSS was not adequately adhered to.

### *Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters*

Although this would seem rather an obvious security measure, it is surprisingly one that many organisations simply failed to comply with. A staggering 81% of the breached organisations had not changed the system defaults throughout their cardholder data environment, including default router configurations, MS Windows guest accounts, shopping cart and website administration interface passwords. Additionally a point of failure is leaving the wireless systems set with the default SSIDs or WEP keys and not encrypting console access. Most organisations also had more than one primary function per server.

The continued use of default passwords may be due to laziness or ignorance, and comprehensive lists of these can be easily found on numerous hacker community web sites.

Even Gary McKinnon, when facing trial for unauthorised access into USA agency and Government systems, stated, “It was child’s play to get into US military systems. Many were using blank or default passwords to access their servers’ Netbios operating system.”

## Protect Cardholder Data

### *Requirement 3: Protect stored cardholder data*

To protect stored data, it is vital that organisations make use of protection methods such as encryption, truncation and hashing. Should someone manage to gain unauthorised access into a system, providing that sufficiently strong encryption is in place and that the keys and passwords are not stored (logically) nearby, the data is unreadable and of little use to that person. An important aim of this requirement is to stop merchants storing the card security code post-authentication.

Over 96% of the organisations that had cardholder data compromised failed to meet this requirement, mainly due to the storing of the card security code after the transaction was authorised.

### *Requirement 4: Encrypt transmission of cardholder data across open, public networks*

Another important requirement of the PCI DSS is that sensitive cardholder information must be encrypted during transmission over networks that can be accessed by malicious individuals.

Almost 64% of organisations had ensured acceptable encryption of data over public networks. Although this is not a very high percentage, it was the most widely adhered to security requirement of all the 12 PCI DSS requirements.

This requirement encompasses not only communications to and from web sites (e.g. online retail accepting card payments), but also other areas such as wireless networks, chat and email.

## Maintain a Vulnerability Management Program

### *Requirement 5: Use and regularly update anti-virus software on all systems commonly affected by malware.*

Only 29% of the organisations that suffered a breach of cardholder data maintained up-to-date anti-virus software on relevant systems, and in many cases there was no antivirus installed. In most cases PCs in office systems were protected by a form of anti-virus, but the majority of website hosting servers were not protected at all.

The most common reason given for this was the risk of degrading the server’s performance if anti-virus was installed.

The main problem here is the most likely place where malware could be used to compromise sensitive data is a server rather than a desktop PC.

### *Requirement 6: Develop and maintain secure systems and applications*

Regular patching of programs and operating systems is a vital aspect of ensuring the security of systems. There are well-known websites that report vulnerabilities in software, applications and operating systems. These are often accompanied with exploits of the vulnerability. With such information being freely available it is important that organisations regularly protect and update systems. PCI DSS states that “all critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.” A significant issue highlighted with patching and updating systems particularly in a Windows environment is the necessity to reboot the server to complete the update. Therefore, causing downtime and potential loss of earnings.

The failure of 100% of the breached organisations to comply with requirement 6 is one of the most telling. Not one of the organisations that suffered a compromise of cardholder data had systems and applications that could be considered secure. Further, in 60% of these, applications vulnerable to SQL injection were used directly or indirectly as part of the successful attack. In 31% of cases, malicious scripts known as web shells were uploaded to gain access to web servers (often via SQL injection). An often overlooked part to this requirement is that generally web developers fail to update their web sites, shopping carts or hosting platforms.

## Implement Strong Access Control Measures

### *Requirement 7: Restrict access to cardholder data by business need-to-know*

As mentioned in the discussion of requirement 3, encryption can serve as a great protector of data, but it does not replace the need for only storing information that is necessary. Requirement 7 then considers that once data is stored, an effective access control policy is in place. Authorisation is increasingly important to both minimise risks of a data compromise, and analysis of the cause of a breach after an event has taken place. The requirement is designed to ensure that sensitive data can only be accessed by authorised personnel. It requires that systems and processes must be in place to limit access based on need-to-know and according to job responsibilities.

Of the organisations that suffered a compromise of cardholder data, just under 31% restricted access to cardholder data on a business need-to-know basis.

Of the cases where the source of the breach was found to come from either inside the organisation itself or from a business partner, 75% of these organisations failed to restrict access in accordance with this requirement.

### *Requirement 8: Assign a unique ID to each person with computer access*

To assist in any investigation after a breach, the assignment of a unique ID to each person with access ensures access to data can be traced to known and authorised users. It also ensures that each user is aware that they are held uniquely accountable for his or her actions.

In over 96% of these cases where cardholder data was compromised, computer access was found to be shared by more than one person who used the same user ID.

In some cases, where there were different IDs used, the same password was used by every person within the organisation.

### *Requirement 9: Restrict physical access to cardholder data*

Enforcing restrictions on physical access to the cardholder data or systems that house cardholder data is another requirement of the PCI DSS. Physical access could otherwise provide an opportunity for individuals to access devices or data and to remove systems or hard copies.

The requirement to restrict physical access to these systems was met in just over 25% of investigations where cardholder data was breached.

The basic intent for this control like all the other controls in the standard is to maintain confidentiality. Although the majority of breached organisations did maintain tight perimeter physical access, most failed to realise the extent of where cardholder data actually was (i.e. the cardholder data was found to be distributed beyond where they thought it was).

Data classification and distribution to or through third party providers and staff needs to be included in the physical security due diligence practices. This is particularly important for merchants spanning geographical areas where cardholder data is maintained in paper form. This generally gets redistributed through various means including couriers, email and fax.

## Regularly Monitor and Test Networks

### *Requirement 10: Track and monitor all access to network resources and cardholder data*

By tracking and monitoring activity on, and access to, network resources and cardholder data, unusual behaviours and anomalies can be alerted and thus potentially prevent a breach. If a breach has occurred, this information can also prove invaluable for detection, investigation and damage limitation. Determining the cause of a breach is significantly more difficult without system activity logs.

Of the organisations that suffered cardholder data compromises, none of them had adequately tracked & monitored all access to network resources and cardholder data.

This requirement is crucial for ensuring that measurement tools exist for controlling and evaluating confidentiality. Generally speaking, the organisations mostly only configured logging to capture OS-related functions and forgot to configure the applications associated with the cardholder data environment. Any application or system component involved in any service or transaction process capable of generating logs must be included to meet compliance. Antivirus events, web server logs, database logs and payment application logs all fall under the scope for PCI-DSS and should be able to produce a full audit trail.

### *Requirement 11: Regularly test security systems and processes*

New vulnerabilities that impact security are being discovered continually by both researchers and malicious individuals. The race is always on between those testing systems with honourable intentions, and those with dishonourable intentions.

Commonly, when a vulnerability in a system or program is found by those serving good, it is published so that a fix can be provided.

System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

As with requirement 10, none of the breached organisations that suffered a breach of cardholder data had ever formally tested their security systems or processes to the required standard. The fact that 100% of the organisations had never conducted thorough penetration testing can hardly come as a surprise for obvious reasons.

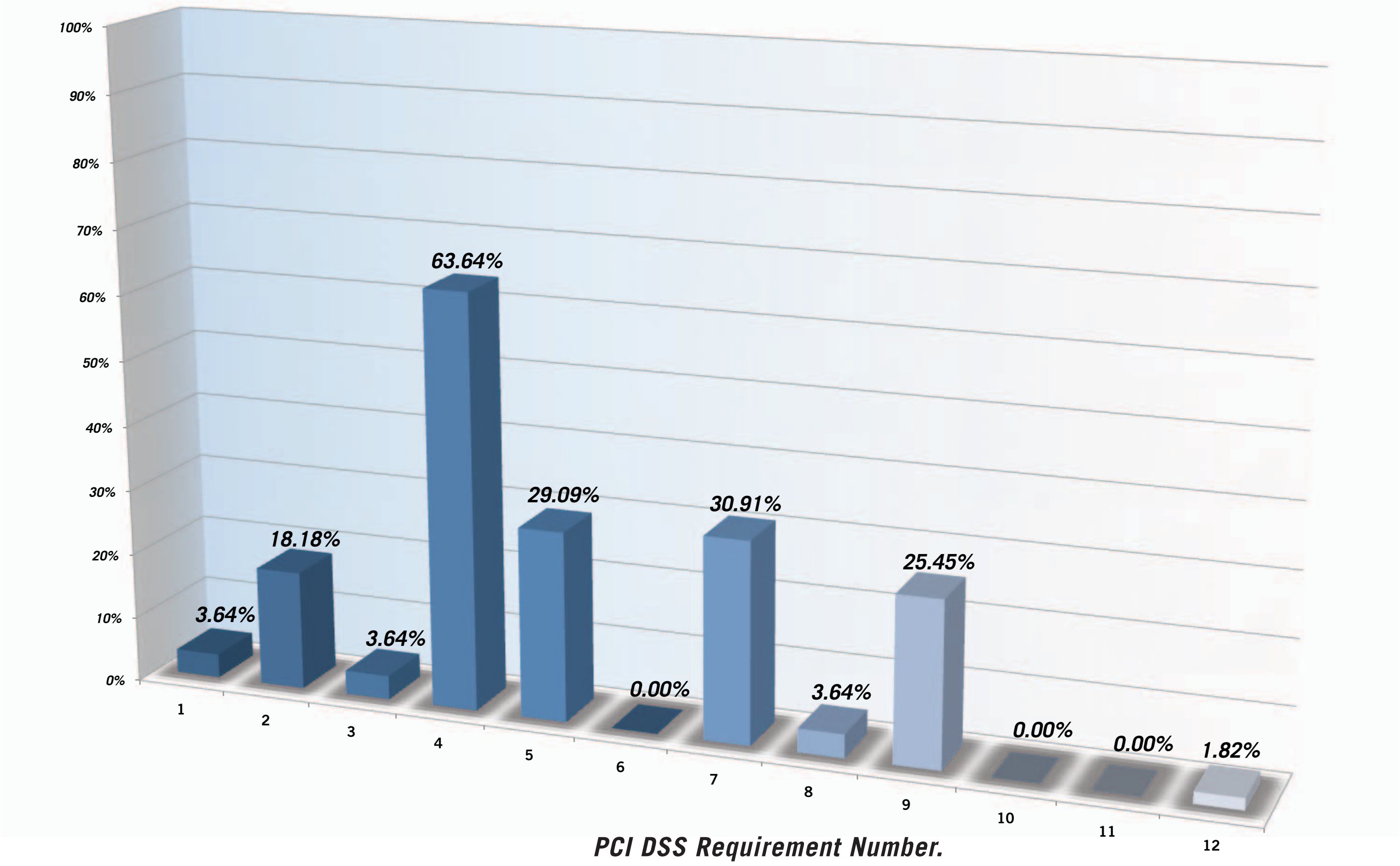
## Maintain an Information Security Policy

*Requirement 12: Maintain a policy that addresses information security*

Clearly, security policies are important to inform employees what is expected of them. All employees should be aware of the sensitivity and value of data and be fully appreciative of their responsibilities for protecting it. The term employees for the purposes of this requirement of PCI-DSS, refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the company's site. In almost all (over 98%) cases investigated where the organisations suffered a breach of cardholder data, there was no adequate information security policy as required by the PCI DSS.

FIGURE 11

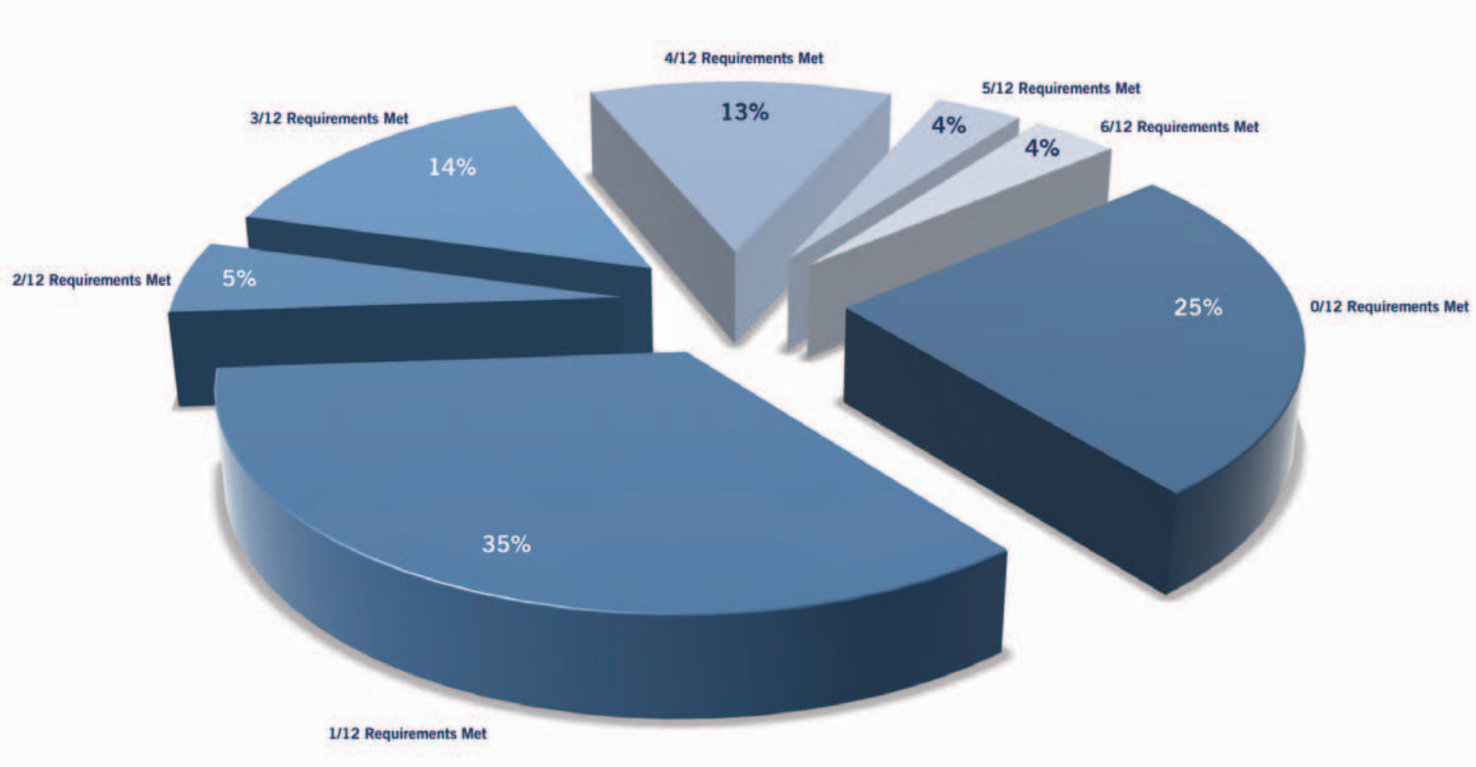
PCI DSS COMPLIANCE



***The percentage of individual PCI DSS Requirements met overall by organisations suffering cardholder data breaches.***

FIGURE 12

PCI DSS COMPLIANCE



***The total number of PCI DSS requirements met (out of a maximum of 12) by the organisations suffering cardholder data breaches.***

Prior to having suffered a cardholder data compromise, 26% of the organisations had believed themselves to be PCI DSS compliant upon submission of completed Self Assessment Questionnaires. The investigations also revealed that none of the organisations met all requirements of the PCI DSS. Indeed, in just over one quarter of the cases, none of the twelve requirements were met. The maximum number of requirements met by an individual organisation was only 6 out of 12, in approximately 4% of cases.

None of the organisations that had satisfied the requirements of PCI DSS Approved Scan Vendor (ASV) vulnerability scanning were sufficiently protected to prevent against being compromised by a combination of attacks that such scanning is purported to detect. ASV scanning is an automated, computer driven task that does not involve human interpretation of results.

An analogy may assist in describing the shortfalls of automated vulnerability scanning. Let us assume that a burglar creates a robot that identifies houses which are easy targets for the burglar to subsequently break into. The robot is programmed to go to the front door of each house, check to see if the door is unlocked, and if it is locked, to look under the door mat for a key.

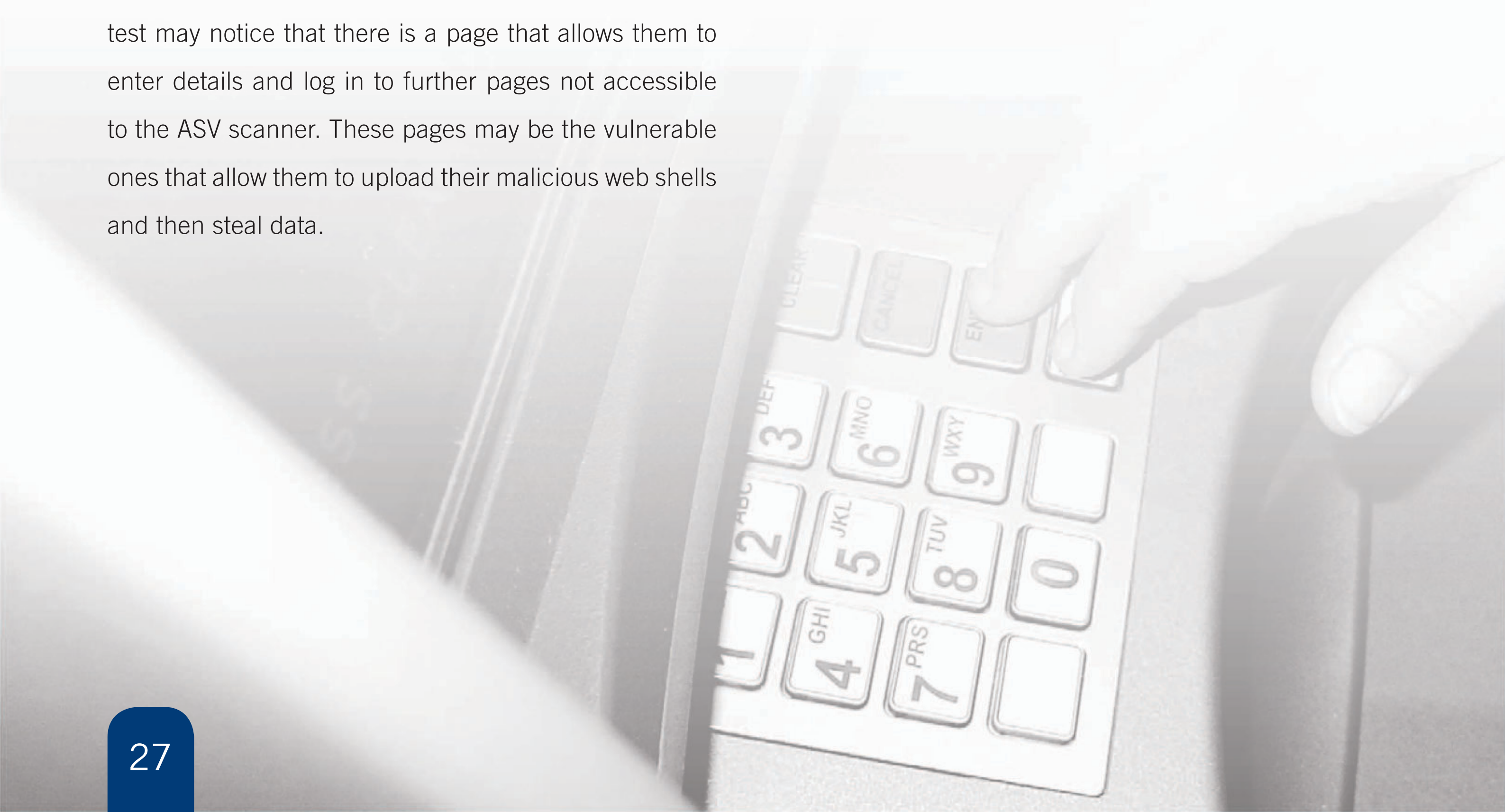
The robot sets off around the neighbourhood and comes across the first house, tries to open the door but it is locked. It then follows the next instruction which is to check under the doormat, but there is no key there. The house is therefore marked as not vulnerable. However, the key was actually sitting on top of the door mat, right in front of the robot, but because the robot was not programmed to deal with this, it missed it.

In this analogy the robot is like the vulnerability scanner, an automated program that will provide some level of checking for vulnerabilities, but with shortfalls. The criminal hackers who break into organisations are not robots and, like the burglar, would have noticed the key sitting there on top of the door mat. This is of course the reason that penetration tests and technical security assessments are carried out by humans.

A common problem found by 7Safe is that an ASV scanner is not "intelligent" enough to sign up or log into website customer user areas. For example an ASV scanner will check for vulnerabilities on the pages it can access at that time. However, a human conducting the test may notice that there is a page that allows them to enter details and log in to further pages not accessible to the ASV scanner. These pages may be the vulnerable ones that allow them to upload their malicious web shells and then steal data.

A significant reason to a merchant not being PCI compliant is not the unwillingness on the merchant's side, but more the lack of understanding and interpretation of the PCI DSS. Often what is needed is a review of the systems by a technically knowledgeable person with a good understanding of the PCI DSS requirements.

7Safe has found that all the merchants who have been subject to a breach and have completed an ASV scan have believed themselves to be secure based solely on the results of this scan, therefore, putting themselves into a false state of security. ASV scanning should not be relied upon in isolation. Further tests, scans and processes should be adopted and used to help understand, locate and prevent the common website vulnerabilities. 7Safe offers these services to their merchant customers and finds that once the merchant understands that the automated scan is different to a trained security consultant using their intelligence and experience to penetration test the website, then more can be done to help secure the website and prevent further attack.



# Conclusions

This report provides detailed information through the analysis of real and current information security breaches.

The analysis clearly reveals that there are certain areas that organisations are commonly found to be neglecting. The high percentage of insecure web applications and susceptibility to SQL injection and malware demonstrates a widespread lack of understanding about these subjects and highlights the need for educating software developers about preventative measures.

In addition, merchants should take further steps to protect their web server environments, conduct security testing and also ask questions of their web developers/ hosting companies who often state that their website has been written securely.

The data also suggests a strong link between security breaches and the absence of thorough security auditing (notably penetration testing and security assessments). The inherent limitations of automated vulnerability assessment tools (that often misrepresent the true state of security of a web site or server) have been clearly highlighted.

The large number of breaches suffered by online retailers can be explained by the potentially lucrative reward of payment card details. Crime has evolved onto the Internet. It may be easier for a criminal to hack into a web server and steal thousands of credit card details and from a hidden location on the Internet, than to steal a purse or a wallet from a vulnerable person to gain some cash and maybe one or two credit card numbers. The risk versus reward has changed dramatically.

The analysis proves that many organisations who declare themselves compliant with the PCI Data Security Standards are not even close. There is often an overwhelming amount of information to comprehend when it comes to PCI and information security for the average lay person. This is completely understandable also; these subjects require very specialist knowledge that is changing on a daily basis, and to expect every ecommerce merchant to understand all points that PCI and information security requires of them without any assistance is going to result in further data security breaches occurring. 7Safe's information security consultants are often asked to support clients who have concerns over the security of their data. This can range from PCI DSS, security assessments, penetration testing and education.

It often falls to the IT Managers and Information Security specialists to implement the technical controls to protect commercially sensitive information.

However, effective information security has a wider remit than that of the IT Manager / Security Specialist. It is the experience of 7Safe that those organisations whose Executive level drives information security as a company-wide managed project are also the most successful in the implementation of effective controls. Therefore we recommend that Company Executives use this report as a catalyst for initiating a review of company wide information security practice and analysis of gaps. IT Managers and Security Specialists should use this report to generate effective business cases to support remediation proposals.

The combined approach of Executive driven, business-led programmes implemented by technically skilled professionals provides a powerful reply to the constant threat to the security of information.

# References

1. Produced by DTI (April 2004). Achieving Best Practice in Your Business
"Information Security: Hard Facts"
Retrieved from:
http://www.berr.gov.uk/files/file9977.pdf

2. Produced by DTI (April 2004) Achieving Best Practice in Your Business
"Data Protection Act"
Retrieved from:
http://www.berr.gov.uk/files/file9979.pdf

3. Produced by DTI (April 2004). Achieving Best Practice in Your Business
"Information Security: Guide to the Electronic Communications Act 2000"
Retrieved from:
http://www.berr.gov.uk/files/file9980.pdf

4. Price Waterhouse Coopers (2006).Information Security Breaches Survey:
"Trustworthy Networking".
Retrieved from:
http://www.pwc.co.uk/pdf/pwc_DTI_TrustworthyNetworking.pdf

5. Price Waterhouse Coopers (2008).Information Security Breaches Survey:
"2008 BERR Executive Summary".Retrieved from:
http://www.pwc.co.uk/pdf/BERR_2008_Executive_summary.pdf

6. Ponemon Institute LLC (April 2009). A study of IT Practitioners in the United States, United Kingdom, Germany, France, Mexico and Brazil.
"Business Risks of a Lost Laptop"
Retrieved from:
http://whitepapers.theregister.co.uk/paper/view/886/the-business-risk-of-a-lost-laptop.pdf

7. Ponemon Institute LLC (April 2009). A Study of U.S. IT Practitioners Sponsored by Dell Corporation
"Business Risks of a Lost Laptop"
Retrieved from:
http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/The%20Business%20Risk%20of%20a%20Lost%20Laptop%20Final%201.pdf

8. Ponemon Institute LLC (2008). Annual Study: "U.S. Enterprise Encryption Trends
Leading IT organizations continue shift to strategic encryption approach".
Retrieved from:
http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008_Annual_Study_US_Encryption_Trends_280308.pdf

9. Ponemon Institute LLC (2008). Report of IT Practitioners in the UK, Germany & France. "Study On The Uncertainty Of Data Breach Detection".

10. Price Waterhouse Coopers for ENISA European Network and Information Security Agency (July 2007). Information Security Awareness Initiatives:
"Current Practice and the measurement of success".
Retrieved from:
http://www.pwc.co.uk/liverpool/pdf/enisa_measuring_awareness.pdf

11. Price Waterhouse Coopers (2008). Information Security Breaches Survey :
"Technical Report"
Retrieved from:
http://www.berr.gov.uk/files/file45714.pdf

12. Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime (1989), Council of Europe.
Retrieved from:
https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2

13. Computer-related Crime: Analysis of Legal Policy (Information, computer, communications policy) (1986), Organization for Economic Co-operation and Development

14. International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime, retrieved from:
http://www.uncjin.org/8th.pdf

15. S.Fafinski, N. Minassian (September 2009) "UK Cybercrime Report 2009"
Retrieved from:
www.garlik.com/press.php?id=613-GRLK_PRD

16. Price Waterhouse Coopers (2009). Online report: "E-espionage: What Risks does your organization face from cyber-attacks?"
Retrieved from:
http://www.pwc.co.uk/eng/publications/e_espionage.html

17. HLSTC PISFU (July 2008) House of Lords Science and Technology Committee, 'Personal Internet Security: Follow Up' 2007-08 HL Paper 131

18. UK Cabinet Office (2008). "National Risk Register"
Retrieved from:
http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx

19. APACS - The UK Payment Association in conjunction with The UK Card Association (2009) "Fraud the Facts"
Retrieved from:
http://www.ukpayments.org.uk/files/publications/exisiting_publications/fraud/fraudthefacts2009.pdf

20. Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry, C. Matthew Curtin, Interhack. Retrieved from:
http://web.interhack.com/publications/interhack-breach-taxonomy.pdf

21. Deloitte (2009). TMT Global Security Survey Key Findings
Retrieved from:
http://www.deloitte.com/dtt/cda/doc/content/nl_nl_TMT_2009_Security_Survey_Findings(2).pdf

- Digital Forensics
- PCI DSS Compliance & Audit
- Penetration Testing
- eDiscovery & Litigation Support
- Data Compromise Investigation
- Security Assessments
- Education & Training Programmes

## Contact Us

Tel: +44 (0)870 600 1667
contact@7safe.com

www.7safe.com