This is an Accepted Manuscript of an article published by Taylor & Francis in Enterprise Information Systems, available online: https://doi.org/10.1080/17517575.2019.1605000

Dying of a Hundred Good Symptoms: Why Good Security Can Still Fail - A Literature Review and Analysis

Paul Loft, Ying He*, Helge Janicke, Isabel Wagner

School of Computer Science and Informatics, De Montfort University, Leicester, UK

Paul Loft

School of Computer Science and Informatics, De Montfort University, Leicester, UK

Email: P15250056@my365.dmu.ac.uk

Ying He*

School of Computer Science and Informatics, De Montfort University, Leicester, UK

Email: ying.he@dmu.ac.uk

Co-responding Author

Helge Janicke

School of Computer Science and Informatics, De Montfort University, Leicester, UK

Email: heljanic@dmu.ac.uk

Isabel Wagner

School of Computer Science and Informatics, De Montfort University, Leicester, UK

Email: isabel.wagner@dmu.ac.uk

Dying of a Hundred Good Symptoms: Why Good Security Can Still Fail - A Literature Review and Analysis

Abstract

Many organizations suffer serious information security incidents, despite having taken positive steps towards achieving good security standards. Security certifications and high levels of maturity may have been obtained, but fundamental security problems remain.

The authors hypothesize that these issues are often as a result of security arrangements not being sufficiently integrated with how the whole organization actually goes about its business. Whether embarking on a new Enterprise Information System (EIS) or refreshing a security strategy, we believe that adopting an enterprise architecture (EA) approach to implementing information security – commonly referred to as an 'Enterprise Information Security Architecture' (EISA) - will deliver substantial benefits. However, EAs typically require specialist resources to develop and maintain them, and this takes time; which makes it difficult for architectures to keep pace with business change. These barriers must be overcome if the EISA is to be effective.

Our paper has reviewed and analyzed literature concerning the root causes of information security incidents and describes a novel approach for ensuring that the most critical factors are considered when building an EISA framework. We propose 8 domains that must be managed together to ensure that an EISA is successful.

Keywords

Information Security; Enterprise Information Security Architecture (EISA); Security Failures

Introduction **and** Preliminaries

The pursuit of innovation and efficiency in modern organizations is undertaken in an environment of increasing complexity, coupled with unprecedented increases in data volumes. Indiscriminately following generic security standards or applying outdated frameworks may not match the risk profiles of organizations, and may not provide adequate protection of information (Sun and Chen, 2008; Wang et al. 2009).

Benchmarking information security key performance indicators (KPIs) against other organizations can be a valuable indicator, and where barriers to protecting such information exist, privacy preserving benchmarking solutions have been described in the literature (Kerschbaum, 2008; Xiong et al. 2017, Zhang et al. 2018). However, accurately specifying static evaluation metrics that will measure security posture for even the most similar organizations faces significant challenges for measurability. Aggregating the dynamic status of information systems to a single metric will lose essential information but conversely, specifying too much detail will make it difficult to determine relevance (Pendleton et al. 2016). Furthermore, applying security standards on a linear scale is unlikely to protect against the full range of vulnerabilities that an organization can face, and will not consider realistic, dynamic attack scenarios.

Adopting the practice of EA in the design and implementation of security strategies will help companies manage complex business processes and support business strategies (Goudalo and Seret, 2009; Wang et al. 2009). In addition to ensuring that routine tasks operate reliably and predictably (Albuquerque et al., 2014; Goudalo and Seret, 2009; Jafarov, 2013), it might also facilitate double-loop organizational learning (Vallerand et al. 2017) in light of the relevant experience being gained throughout the enterprise and, therefore, helping to support valuable transformation initiatives. This could support management to seek out business change opportunities (Tahajod, 2009). Without this level of organizational structure, knowledge of the business could become isolated into silos, with executives initiating business change with a limited perspective on the wider implications for its information security.

Some of the latest advances in technology, such as the Internet of Things (IoT), require that organizations take an holistic view as to how they secure information and services, since these technologies may have least complexity and are unlikely to be innately secure (Adat and Gupta 2018). Senior executives are cognizant of the need to embrace these new

technologies but are not always considering the security risks that these technologies can incur for their business, as security is often traded for usability without due diligence being applied.

Where an organization's data becomes distributed and decentralized, such as in the case of cloud-based services, consideration must also be given to the security arrangements of these services and of their partners that are providing the services (Gupta et al. 2017; Stergiou et al. 2018). The risks from new technology and business change can grow unchecked (Luethi and Knolmayer, 2009), if an organization focuses its information security strategies solely on its traditional systems (Ahmad, 2005; B Farroha and Farroha, 2011; Chen et al., 2012; Tanaka, 2009; Zhidzir et al., 2010). The needs for information security are pervasive throughout the enterprise architecture. Therefore, both business architecture and IT architecture need to be considered holistically in order to select the most appropriate security models (Gupta et al. 2016). Security must not unduly hinder business function, but business processes must have due regard to security constraints, including legislative and regulatory requirements (Atay and Masera, 2011; Li et al. 2018; Ohki et al., 2009). Modern security challenges are comprehensively referenced in *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives (Gupta et al. 2018)*. These studies reinforce the principle that security solutions have to extend beyond traditional boundaries and provide trusted services that help both reduce complexity and increase security.

Existing architecture frameworks typically require extensive knowledge of other standards and concepts, with the skill and time available to selectively incorporate them into the architecture (Kaisler, 2005). Organizations tend to make compromise decisions and depart from the architecture in fundamental ways to deliver faster, but, in the process, rendering the architecture ineffective (Shah and Kourdi, 2007).

Our paper has reviewed and analyzed literature concerning the root causes of information security incidents over a 10 year period since EISA's became commonly established, and has considered whether an enterprise architecture approach for information security was identified in the literature. Analysis of the literature was conducted using a mixed method of quantitative and qualitative research.

This paper aims to test the authors' hypothesis that security failures can result from a lack of consideration for the full characteristics of the enterprise when defining information security strategies. As such, it seeks to answer the following research questions:

(RQ1) To what extent do the root causes of information security incidents relate to potential failings in how an enterprise has implemented its information security programs?

(RQ2) To what extent has enterprise architecture already been seen as a potential solution to make information security more effective?

(RQ3) Are there any fundamental differences between the public and private sectors that need to be taken into consideration when taking an EA approach to information security?

We describe the methodology of our systematic literature review in Section 2 and present our findings in Section 3, focusing on the quantitative analysis in Section 3.1 and the qualitative thematic analysis in Section 3.2. We discuss the value of enterprise information security architectures in Section 3.3 and differences between the public and private sectors in Section 3.4. We then discuss our general findings in relation to our original research questions in Section 4, and conclude the paper in Section 5.

Methodology

This study is divided into i) a review of the root causes of security incidents, both in the

context of IT security failure and success criteria, and ii) a review of the benefits of enterprise information security architecture implementations. Our literature review followed a systematic approach according to the principles set out by Kitchenham and Charters (2007). This consisted of defining the search plan; specifying inclusion and exclusion criteria; selecting keywords for the search; creating Boolean search strings; selecting the analysis method(s); selecting the literature; and finally, analyzing and synthesizing the data.

Literature search

Figure 1 shows our search keywords. We created two separate collections, described throughout the review as non-targeted (i.e. root causes, top half of Figure 1) and targeted (i.e. architecture implementations, bottom half of Figure 1). Searches were restricted to article meta data and abstract only. All papers were selected and analyzed by the lead author, who is a practitioner in IT security.

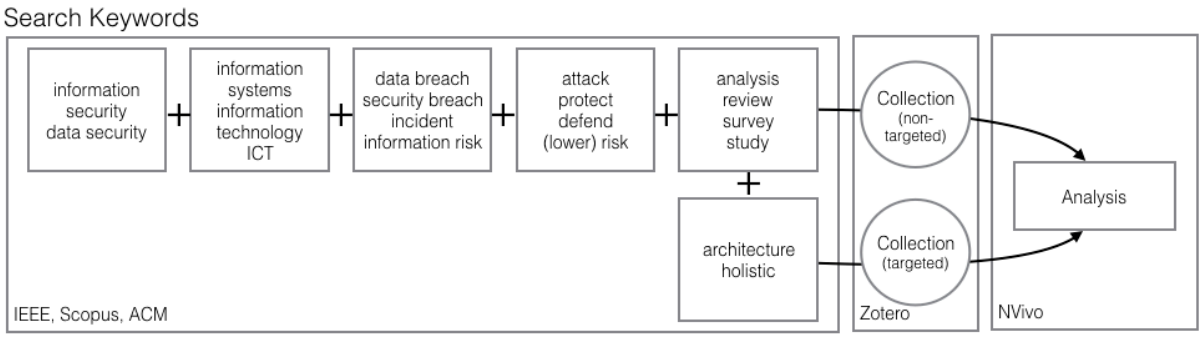

Figure 1 - Literature search: shows keywords used by the authors to search for literature.

Our search criteria was specifically designed to discover detailed academic studies of information security incidents, as opposed to facilitating the creation of a taxonomy of the technical nature of attacks.

Inclusion and exclusion criteria

Enterprise Information Security Architecture, as a concept, started to gain recognition around

2005 (Gartner, 2017; Shariati et al., 2011). We therefore restricted the search to the last ten years (2005 to 2016). We excluded articles that are not written in the English language, older articles that had zero citations, and non-academic papers.

Analysis method

The search identified 62 articles for detailed analysis. They were read in full and coded in NVivo (QSR NVivo version 10, 2014), to provide statistical data for the quantitative analysis. We then examined the correlations between the codes and their impact on the success or failure of IT security initiatives. We created NVivo nodes dynamically as the articles were read in full. This ensured that the root causes of security failures and successes were captured with an appropriate level of granularity. Nodes were created on the basis of evidence of failures or successes, rather than future predictions. In total, we created 65 nodes that capture potential root causes of success or failure of information security. In addition to nodes for root causes, we created additional nodes to indicate whether the reference described a cause of failure or success, and whether the reference was specific to the public or private sector (where the distinction could be made reliably). We conducted both quantitative analysis of the individual coding and qualitative analysis of the nodes created. The results of these processes are described below.

Findings

Quantitative analysis of the coding

Our quantitative analysis studies dependencies between the 65 nodes we identified during the coding. Figure 2 shows the total number of references for each node. *Human Factors* and *Risk Management* are referenced the most.

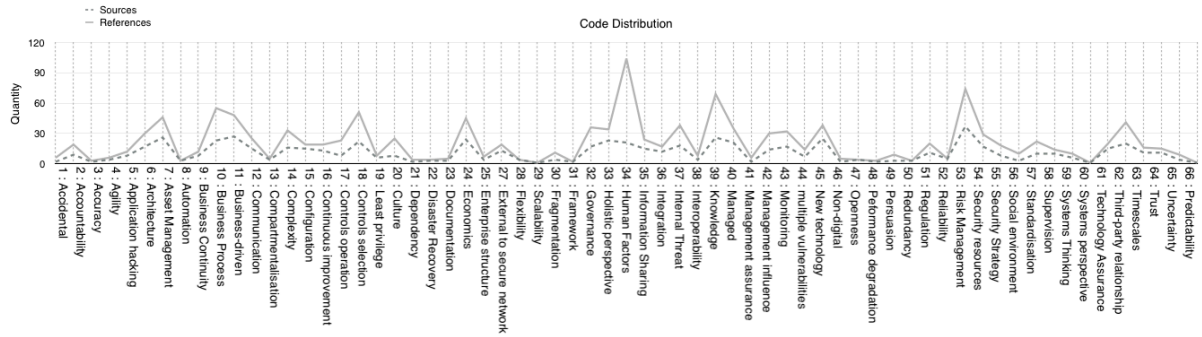

Figure 2 – Code distribution: shows the frequency of coding.

However, the true extent to which each node corresponds to instances of failure or success of IT security is given more precisely by correlation values instead of reference counts. The correlation coefficients between the root cause nodes and their corresponding *success* or *failure* nodes indicate the extent to which each node influences the success or failure of IT security within our study.

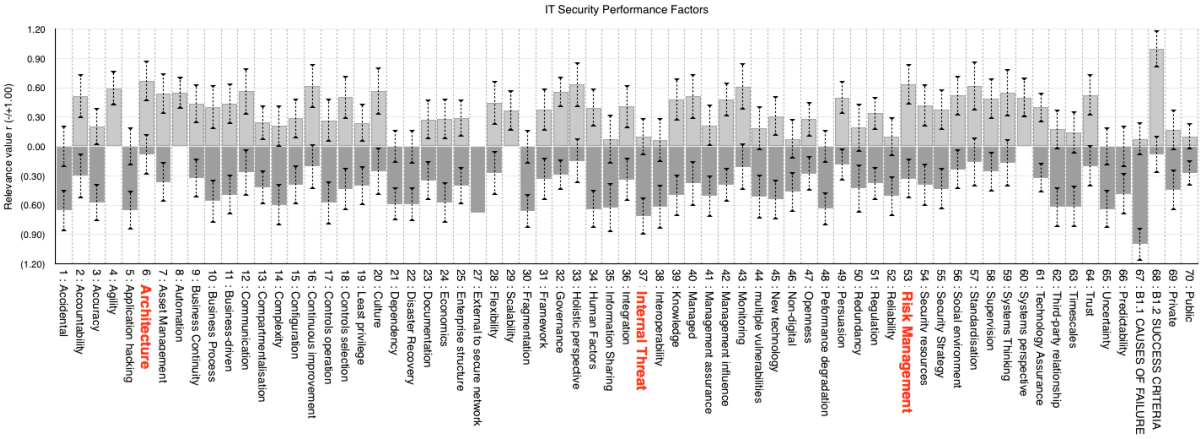

Figure 3 – Node failure/success correlation: shows how each node correlated with success or failure of security.

Figure 3 shows the correlation coefficients associated with success (light grey, upper half) and failure (dark grey, lower half). The error bars indicate the standard deviation of all nodes' correlation values. The figure shows that, while ***Risk Management*** is one of the most frequently mentioned factors, it is mostly attributable to the success of information security, rather than failure. We can also see that ***Architecture*** (r=0.67) is the most significant factor of

success, and that ***Internal Threat*** (r=0.71) is the most significant factor in the failure of IT security, or in other words, the cause of security incidents.

However, it is necessary to investigate these correlations further to determine the root causes. We therefore analyzed how nodes correlated with each other by computing a pairwise correlation matrix. The result, a matrix of 4,225 cells (65x65), is shown in Figure 4.

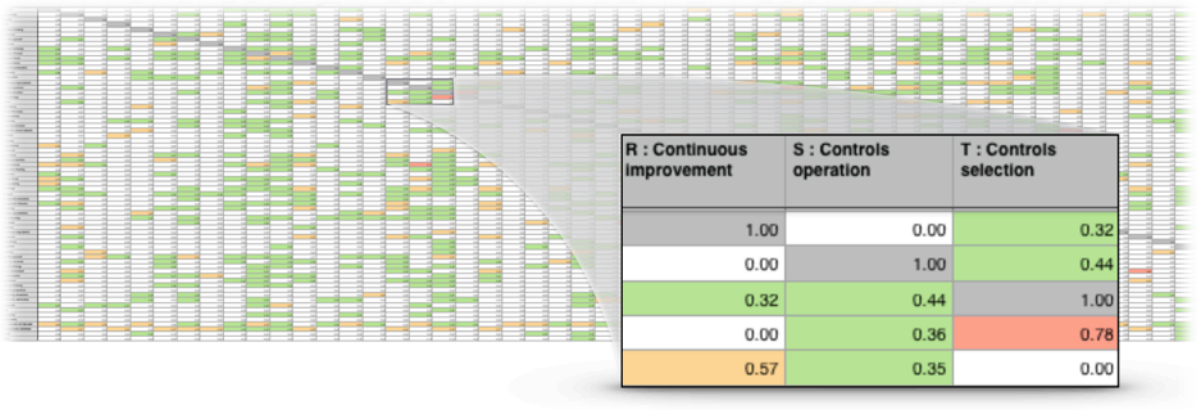

Figure 4 - Pairwise correlation matrix; shows a sample of the matrix.

Following the strongest correlation coefficients in this matrix highlights a chain of events or activities that frequently work together. For example, *Human factors* is associated with the *Internal Threat*; which needs *Supervision*; to enforce *Accountability*; and build *Trust*; in *Third Party relationships*. This chain is highlighted by the green, dotted lines in Figure 5. Therefore, to help reduce *Human Error*, we would most likely need a continual review of our business partner arrangements. Similarly, *Documenting* security *Knowledge* into repeatable *Business Processes* can also help to reduce *Human Error*. These links or chains form the foundation of our analysis. Figure 5 shows each node with its strongest correlation.

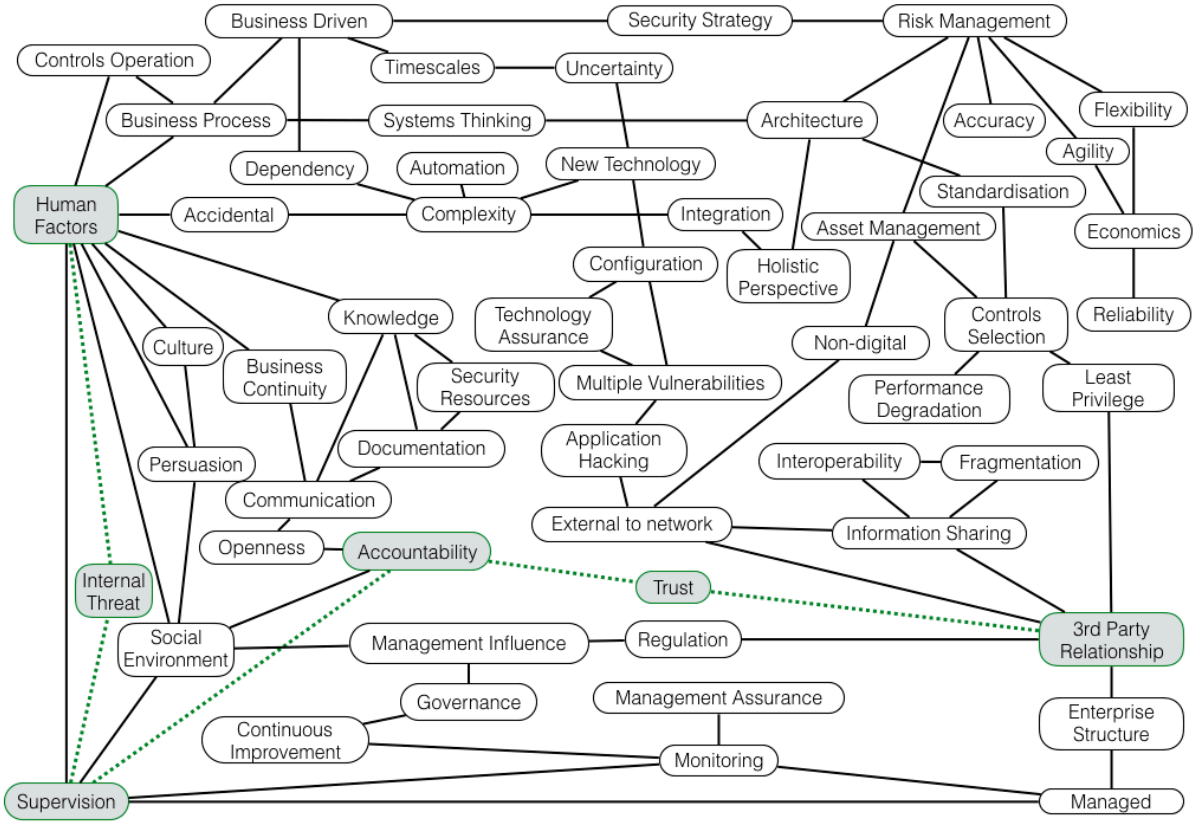

Figure 5 - Strongest node pairs: shows the strongest pairing of the node to node correlations.

Figure 6 shows the nodes in an X-Y scatter chart, which provides a different perspective of the same information. Nodes are positioned in relation to their overall effect on success or failure and their correlation with other nodes.

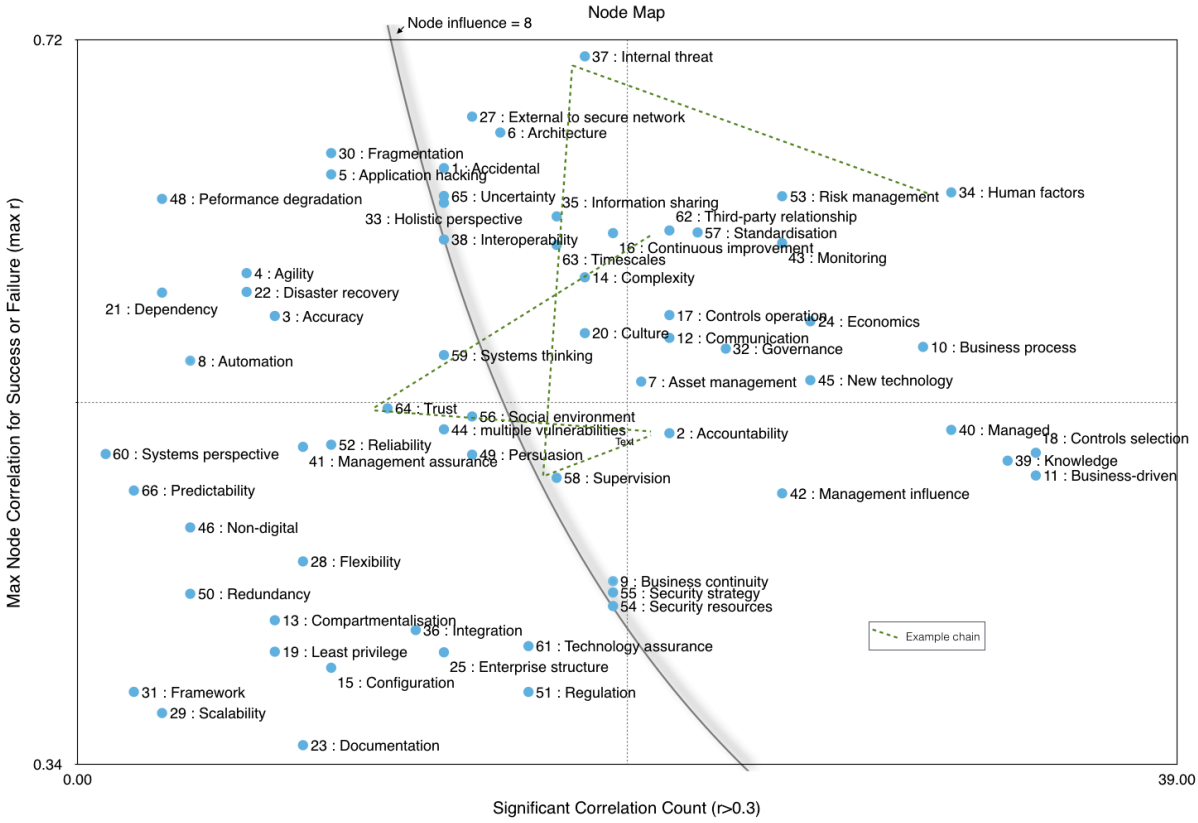

Figure 6 - Node Influence scatter chart: plots nodes based on their correlation to success and failure, and of their correlation to each other.

The nodes in the bottom-right quadrant have a significant correlation with many other nodes, but only a weak correlation with success or failure. This often means that, while they are not one of the highest contributors to success or failure, they are a significant contributor to the success or failure of other nodes, for example *Business-Driven*, or *Knowledge*. For the top-left quadrant, the reverse is true. The nodes in the upper right quadrant show both a high correlation to IT Security performance, and a high correlation with other nodes, with *Human Factors* being the most influential. The graph shows that the relationship is non-linear, and the key relationships between nodes are complex (the green, dotted line highlights the nodes in the earlier example).

Qualitative Analysis of the Nodes

We used inductive (bottom up) Thematic Analysis (Braun and Clarke, 2006) to explore the node references. This method of qualitative analysis allowed us to make the most impartial analysis based on the data that we collected from the articles. Our analysis was conducted by referring to the source references to analyze the coding and determine the themes. This process ensured that the themes were predominately influenced by the articles rather than a preconception of any architecture that the findings might be aligned to. Eight high-level themes were identified through this process in which all nodes could be grouped by shared characteristics. All 65 nodes are grouped under these 8 themes, and we refer to the themes as domains. They are: Business Process (BP); Enterprise Architecture (EA); External Factors (EF); Human Factors (HF); Information Assets (IA); Management Influence (MI); Security Governance (SG); and Technology Infrastructure (TI).

When determining the domains, we primarily focused on the most influential nodes. Figure 7 shows that the eight domains identified are widely represented in the upper right quadrant of the node influence scatter chart.

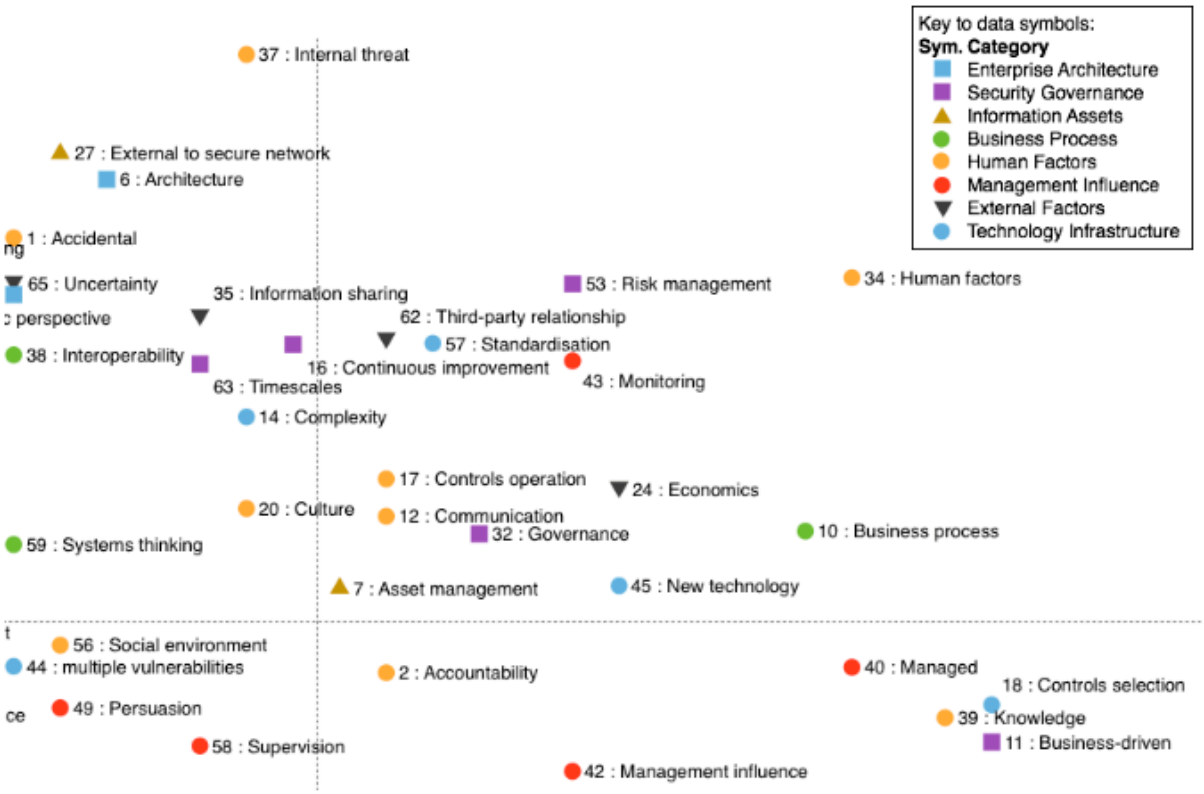

Figure 7 - Most influential nodes: shows how the most influential nodes are widely represented by the 8 domains.

For our analysis of these domains, we first calculate the influence that each node has on the performance of IT security, both in terms of its own impact on success or failure, and in terms of its influence on other nodes. We define this influence as the product of its correlation to success/failure (whichever is greater) and the number of other nodes that it has a significant correlation with. Since r values of less than 0.3 are considered to have little correlation (Asuero et al., 2006), we only count nodes with $r \geq 0.3$. We therefore calculate the influence for each node i as follows, with j denoting the nodes except i:

$$influence_i = \max(r_{i,success}, r_{i,failure}) \times |j|, where\ r_{i,j} \geq 0.3$$

This influence corresponds to the area that each node delineates in the scatter chart (Figure 6), when drawing a rectangle from the graph origin. The resulting influence values are between 0 and 20, with 20 being the most influential (i is in [0.3,1] and j is in [1,65], with 34 being the highest actual node count for $r \geq 0.3$).

For this paper, we select nodes that have an influence value ≥8.0, because that is the median of all node influence values. A line is shown in Figure 6 that represents an influence value of 8.0. Statistically, the median is the most likely influence value for a given node, and is less likely to be affected by abnormally high or low values.

Figure 8 shows the relationships between the domains in a cobweb diagram to aid further analysis. The thickness of the links represents the strength of the correlation values.

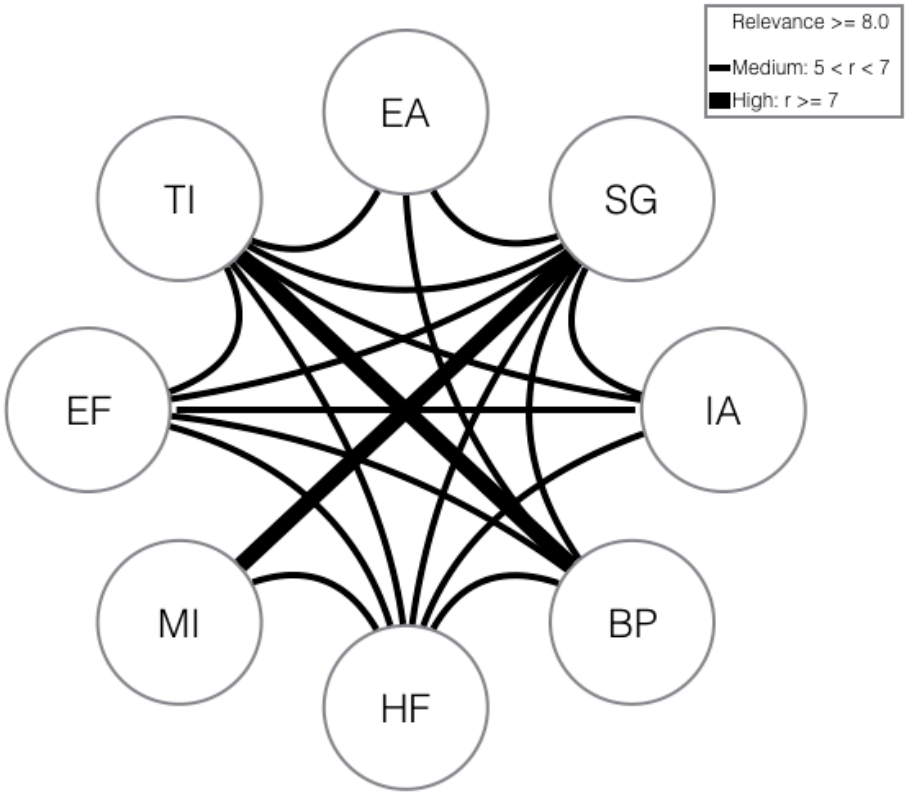

Figure 8 - Domain Cobweb: shows the strongest correlations between the domains.

We describe the 8 domains below. We start with Information Assets, since the application of information security should start with an analysis of the information processed by the business (Ahmad, 2005; Bahmani et al., 2010; Bottino, 2006; Dzazali et al., 2009; Goudalo and Seret, 2009; Luethi and Knolmayer, 2009; Michelberger and Lábodi, 2012; Ohki et al., 2009; Polstra III, 2005; Shaikh, 2005; Soomro et al., 2016; Tsaih et al., 2008). We then describe the other domains in an order that roughly follows the correlation between the domains.

Information Assets

Category	Node	Node influence
Information Assets	Asset Management	10.81
	External to secure network	9.51

Table 1 – Information Assets

The **Information Asset (IA)** domain is a crucial starting point for identifying how to apply information security. Overall, the IA domain has a strong correlation with the failure of information security (r=0.57). This is partly due to the poor management of assets leaving the secure network (**external to secure network**) (Ahmad, 2005; Chen et al., 2012). This is reflected in the strong correlation with the **External Factors** domain, particularly for its **information sharing** (r=0.69) node. These findings are described further in the next section.

However, when the **asset management** node is correlated with other nodes, it shows a positive correlation with the success of information security, and it appears in the top right quadrant of the scatter diagram (see Figure 6). The strongest correlation is with **risk management** (r=0.63).

An architecture requires determining what assets are important to an organization and their true value (Goudalo and Seret, 2009), and this is often achieved by determining the sensitivity of data before conducting risk assessments (Bottino, 2006). This ensures that the

cost-benefits of security solutions can be evaluated before procurement and implementation, and that only the necessary level of security is applied. **Risk management** node is part of the **Security Governance (SG)** domain and is discussed in more detail in a later section.

External Factors

Category	Node	Node influence
External Factors	Economics	14.88
	Third-party relationship	13.02
	Information Sharing	10.66
	Uncertainty	8.29

Table 2 - External Factors

There are several **External Factors (EF)** that greatly influence the success or failure of information security, and the **economics** node is the most significant (r=0.57). Whilst the literature review did identify economic factors that were associated with security threat - particularly the **internal threat** (Duncan and Whittington, 2015; Shropshire, 2009), our objective was to identify the effects on vulnerabilities. **Economic** pressures often lead to organizations taking greater security risks (Birman, 2006), as systems can be built and launched without appropriate consideration for security (Collmann and Cooper, 2007; Park et al., 2010), or limited budgets are not being spent on the right security controls (Sen and Borle, 2015). There are significant differences between public and private sectors (Choo, 2011) (see Section 0).

Third party relationships are often established without sufficiently robust contracts (Luethi and Knolmayer, 2009), that lay down security expectations and responsibilities (Cooper, 2015; Li and Hongyan, 2010; Zhidzir et al., 2010). Consideration for information security activities must feature highly in the selection of third parties (Ohki et al., 2009), and in the design of systems that are used by third parties, to ensure that control of information assets is maintained (Lalanne et al., 2013; Zhidzir et al., 2010).

Information sharing with business partners can bring significant business advantages, but as traditional network boundaries become extended, the security of one organization can have a significant impact on another (Tanaka, 2009). Unsecure methods of data sharing are one obvious concern (Azmi, 2012), but secure connections are just one part of the risk, and strict 'need-to-know' principles need to be robustly embedded in information systems (Atay and Masera, 2011). Evidence shows that this can be a retrospective process, as development priorities do not adequately consider interface requirements (B Farroha and Farroha, 2011).

The pace of development and the complexity of technology architectures to support collaboration leads to **uncertainty** that information security is appropriately addressed (Dzazali et al., 2009). This is a key reason why the EF domain has a strong correlation with the **Technology Infrastructure (TI)** domain, and this is discussed further in the next section.

Technology Infrastructure

Category	Node	Node influence
Technology Infrastructure	Controls selection	17.12
	New technology	14.08
	Standardization	13.62
	Complexity	10.72

Table 3 - Technology Infrastructure

We placed the highest number of nodes in the **Technology Infrastructure (TI)** domain (17 in total), and on average TI nodes showed the greatest correlation with success or failure. Table 3 lists the nodes that are in the TI group for node influence values of 8 and above.

By examining these high-relevance TI nodes, it was evident that poor **controls selection** will defeat any other security measure (Luethi and Knolmayer, 2009). Security needs to be developed into the technical architecture, and this becomes more important as networks grow and become more **complex** (Bottino, 2006).

Organizations can be exposed to greater risks when they adopt **complex** and unfamiliar

technologies (Dzazali et al., 2009). It is therefore preferable to phase the adoption of **new technology**, to ensure that it is properly understood, and that adequate resources are in place to support it.

As can be seen from Figure 8, the domains that have the strongest correlation with TI are the **Business Process (BP)** and **Human Factors (HF)** domains.

Implementing technology in a disorganized way, without **standardizing business processes**, will eventually result in a negative impact on security (Collmann and Cooper, 2007). For example, interfacing with external processes and organizations is often considered as secondary to the internal requirements of an information system (B Farroha and Farroha, 2011; Dzazali et al., 2009), but it is also difficult to add this functionality later in a secure way. There can be a trade-off between providing **interoperability** as quickly as possible, and doing so securely. This is where enterprise **security architectures** can provide clear benefits and provide **accountability** (Bahmani et al., 2010).

It is also important that the **controls selected** are appropriately matched to the criticality of the data to be protected, with only the necessary amount of security implemented to control costs and ensure that the architecture of the network is easy to maintain (Bottino, 2006; Dzazali et al., 2009).

When implementing and configuring technology, **human factors** will always have an impact on the success of information security. For example, when selecting security controls, enforcing the **least privilege** principle will reduce security vulnerabilities (Azmi, 2012; Brunette Jr and Schuba, 2005; Luethi and Knolmayer, 2009; Martin and Rice, 2011; Zhidzir et al., 2010).

Business Process

Category	Node	Node influence
Business Process	Business Process	16.77
	Business Continuity	8.29
	Interoperability	8.00

Table 4 - Business Process

The **business process** node has a high influence value (r=16.77), and this is mostly attributed to the large number of significant correlations that it has with other nodes (30). As can be seen from Figure 8 - Domain Cobweb, there is a strong correlation between the **Business Process (BP)** domain and the **Technology Infrastructure (TI)** domain, and implementing security technology can be a futile effort if this is not accompanied by clear working practices (Dzazali et al., 2009), and automating these working practices is an indicator of the level of maturity in organizations (Brunette Jr and Schuba, 2005).

The BP domain is also linked to the **Human Factors (HF)** domain and it is important to have user involvement when information security is built into business processes (Waly et al., 2012). Making information security central to the design of business processes reinforces a good security culture (Alumark et al., 2015). It also provides a valuable understanding of how new technology will be operated in practice (Whitman and Mattford, 2012), and highlights if previously selected controls are not the most appropriate (Ahmad, 2005).

Ensuring that there are standard processes in place to recover from security incidents, and that these are constantly tested and adapted by trained personnel, are also key to maintaining **business continuity** (Dzazali et al., 2009; Renato and Maria, 2015). Poor connectivity solutions to maintain **interoperability** in a complex IT infrastructure can allow errors to quickly transfer from one system to another (Collmann and Cooper, 2007; Sommestad et al., 2009) and harm an organization's ability to quickly recover services in the event of a failure (Luethi and Knolmayer, 2009). This is further complicated by multiple vendors who do not

support common standards of information security and require unsecure workarounds, such as copying data out of directory services (Luethi and Knolmayer, 2009). Careful design is required to balance the needs of **interoperability** and information security (Bahmani et al., 2010).

Control of the **business process** is strongly correlated with **Enterprise Architecture**, and this is discussed in the next section.

Enterprise Architecture

Category	Node	Node influence
Enterprise Architecture	Architecture Holistic Perspective	10.07 8.25

Table 5 - Enterprise Architecture

There are two nodes in the **Enterprise Architecture (EA)** domain with a node influence value of 8 and above, and this is attributed to their direct association with the success of information security programs (see Figure 3 and Figure 6).

As we describe in our thematic analysis, security incidents require multi-pronged action (Azmi, 2012). Common architectures provide this by default, by ensuring that technology, the business goals, the processes and information flows, and the people of the organization are equally considered (Dzazali et al., 2009; Soomro et al., 2016). In other words, **architectures** enforce a **holistic perspective**.

Building technology by following a sound **architecture** makes the infrastructure easier to understand and support (Bottino, 2006; Park et al., 2010). An architecture provides a top-down approach to understanding the enterprise and informing the selection of security controls (Andrews et al., 2014; B Farroha and Farroha, 2011; Goudalo and Seret, 2009; Mukundan and Sai, 2014; Ohki et al., 2009; Soomro et al., 2016). In this way, expenditure on security solutions is easier to justify.

An **architecture** also allows organizations to quickly assess the impact of new vulnerabilities discovered within the infrastructure (Andrews et al., 2014; Fenz et al., 2008), and helps organizations provide business continuity (Soomro et al., 2016). Importantly, the **architecture** itself must be easy to maintain, since it will be constantly changing (Fenz et al., 2008), and must be continually updated to the specific needs of the organization (Soomro et al., 2016).

In addition to the **Business Process (BP)** domain, **Enterprise Architecture** is also strongly correlated with **Security Governance (SG)**. **Enterprise architectures** provide a suitable **framework** in which to achieve many of the benefits described above (Brunette Jr and Schuba, 2005). Whilst the **framework** node itself does not achieve a high influence value (it is bottom-left in Figure 6) and therefore not included in our description of the **Enterprise Architecture** domain, it does have a strong correlation with the **risk management** node, which is a key to **Security Governance**.

Security Governance

Category	Node	Node influence
Security Governance	Business-driven	16.71
	Risk Management	15.95
	Governance	12.83
	Continuous improvement	11.75
	Timescales	10.41
	Security strategy	8.17
	Security resources	8.04

Table 6 - Security Governance

Table 6 shows that the **Security Governance (SG)** domain contains many nodes with a significant influence on the success of information security. Figure 8 shows how the SG domain has strong correlations with all other domains. In fact, the combined nodes in SG have a higher average correlation with other nodes (r=0.41) than any other domain. A **business-driven** strategy has the largest influence on successful **Security Governance** (16.71), but according to Ernst & Young, 85% of information security programs are not

fulfilling business needs, and 62% do not align information security to enterprise architecture or the business process (Iguer et al., 2014).

Security for security's sake has limited value to the business, and the organizational context determines the effectiveness of an information security strategy (Park et al., 2010). Conducting accurate risk assessments requires consideration for the changing business environment, as well as the technical environment (Sommestad et al., 2009). Assessing the risks to corporate information needs to feature as a key aspect of wider corporate **risk management** (Singh and Lilja, 2009) and extend across these boundaries (Brunette Jr and Schuba, 2005), but the pace of technological advancement can often mean that technologies are implemented without a full understanding of the risks to the business (Atay and Masera, 2011).

An effective information **security strategy** requires a constant reassessment of information security risks and the **continuous improvement** of controls (Atkinson et al., 2006; Michelberger and Lábodi, 2012). This is the familiar Deming Cycle, or PDCA (plan–do–check–act) cycle (Ohki et al., 2009), and requires that the **security strategy** is sufficiently dynamic to keep pace with the rate of business and technological change (Dzazali et al., 2009). Brunette et al. (Brunette Jr and Schuba, 2005), describe four transformational phases of "consolidation, standardization, automation, and optimization". Organizations progressing through these phases will realize the "security, agility, and efficiency benefits afforded by the systemically secure architecture approach", thereby increasing their levels of architectural and operational maturity in relation to IT security.

However, such as strategy requires both an understanding of business/human factors, along with sound technical knowledge and experience. The high cost and lack of availability of competent **security resources**, particularly those with technical knowledge and experience,

can make this prohibitive for some organizations (Dzazali et al., 2009).

Security Governance must also consider corporate **timescale** pressures. Technical project teams are often psychologically driven to shortcut security standards to meet the demands of business executives, despite knowing that their actions might contravene security policy (Collmann and Cooper, 2007).

These issues highlight a significant challenge for **Security Governance**. The **Security Governance** domain is highly correlated with the **Management Influence (MI)** domain, and this is described in the next section.

Management Influence

Category	Node	Node influence
Management Influence	Managed	15.98
	Monitoring	15.33
	Management influence	12.05
	Supervision	8.33

Table 7 - Management Influence

The **Management Influence (MI)** domain has a very strong correlation with the **Security Governance (SG)** domain, but many organizations are not **managing** their information security risks, and in some cases, have not fully identified them (Brunette Jr and Schuba, 2005). A failure of **management** to assign responsibility for the ownership of corporate information (Zhidzir et al., 2010), or to understand how their business operates (Polstra III, 2005), can often be at the root cause of security breaches.

The quality of executive support and continuous **monitoring** are significant factors in achieving successful information security (Soomro et al., 2016). Unfortunately, most executives regard information security as an administrative matter (Ohki et al., 2009), but the **Management Influence** domain has a strong correlation with the **Human Factors (HF)** domain. Good security cannot be commanded; it must be "shaped and directed" (**influenced**)

(Herath and Rao, 2009; Sherif et al., 2015). Without this commitment, business leaders are unlikely to achieve the results that they desire (Mukundan and Sai, 2014). While training is arguably one of the most important factors compared to other security measures (Soomro et al., 2016), it is only one part of a wider security program (Martin and Rice, 2011). Employees must be encouraged to transfer their security awareness training to the work place (Waly et al., 2012).

In an analysis of motivation and deterrence (Herath and Rao, 2009), it was found that employees may not always know what the organization's expectations are. It confirms employee negligence as a cause in many costly security breaches but suggests that employees often regard security policy as discretionary, more like guidelines, and may choose not to comply with security policies for reasons of convenience. Employees are also influenced by the attitudes or actions of their peers (Herath and Rao, 2009). The pressure to comply with these subjective norms (e.g. "well, everyone does it this way") can be greater than what people truly believe is right or wrong. Without **supervision**, employees may not be motivated to follow security policies and procedures, so they might as well not exist (Waly et al., 2012). This is significant because employees, when left to themselves, often underestimate the security risks associated with their actions, such as transmitting personal information insecurely (Mukundan and Sai, 2014).

Human Factors

Category	Node	Node influence
Human Factors	Human Factors	19.84
	Knowledge	16.48
	Internal Threat	12.80
	Controls operation	12.09
	Communication	11.84
	Accountability	10.79
	Culture	10.19
	Accidental	8.48

Table 8 - Human Factors

The **Human Factors (HF)** domain contains the individual node with the highest influence on the success or failure of security programs (19.84). It is also the domain with the highest number of node influence scores above 8 (see Table 8) - it occupies the top right hand position in Figure 6.

Knowledge has a high relevance value and this is mostly due to it having the highest number of medium correlation values with other nodes (11 in total). For example, security policies are sometimes constructed without a full appreciation of how the business operates, and this can lead to gaps in the policy, or damage to user confidence, because users simply cannot comply (Duncan and Whittington, 2015; Polstra III, 2005; Whitman and Mattford, 2012).

The **internal threat** is the most significant aspect in security failures (see Figure 3). Legitimate users can cause data loss, either **accidentally** or maliciously (Polstra III, 2005). Perhaps the most obvious reason for this are the failures in **controls operation** by users, such as sharing passwords (Azmi, 2012; Luethi and Knolmayer, 2009), or sharing/losing portable devices (Guha and Kandula, 2012), but also insufficient attention is often paid to the **human factor**, when designing information systems (Zhidzir et al., 2010). Human errors can often occur due to the environment that employees operate in, and mistakes are often made in stressful working environments (Zhidzir et al., 2010).

A good security **culture** needs to be carefully shaped and directed (Sherif et al., 2015). Personality types can affect how compliant individuals will be in terms of following security policy and a study by Johnston et al. (2016) has shown that different levels of emotional stability can affect how individuals decide to take risks in relation to compliance with security requirements. Therefore, the performance of individuals in terms of supporting the organization's desired security **culture,** and their understanding of the social norms (Herath

and Rao, 2009), is something that requires continuous assessment (Duncan and Whittington, 2015; Sherif et al., 2015).

Communication has a strong correlation with success/failure and with other nodes, and several of these nodes are associated with the **Management Influence** (MI) domain (see correlation in Figure 8 and the MI Domain description above)**.** Whilst management may communicate the message that information security is everyone's responsibility, they may be cultivating an environment in which it is no one's responsibility, as there is no **accountability** (Dzazali et al., 2009). The importance of management influence on human behavior was previously highlighted by Tsohou et al. (2015) as a key organizational influence on employees' attitudes.

The HF domain has a strong correlation to the **Technology Infrastructure (TI)** domain. In our study, this was particularly associated with **selecting controls** that provide **least privilege**, such as role-based access control (RBAC) (Brunette Jr and Schuba, 2005; Luethi and Knolmayer, 2009; Zhidzir et al., 2010).

The value of Enterprise Information Security Architectures (EISA)

Our literature review showed that architectures help to simplify the complexity of information security strategies in many ways, for example by providing a framework that can easily be followed (Park et al., 2010) and allow for multi-pronged action (Azmi, 2012). Security must be engineered into every aspect of the network design (Bottino, 2006), but future research must not just focus on technology, but must consider the business goals, the processes and people of the organization (Dzazali et al., 2009; Soomro et al., 2016).

Building technology by following a sound architecture makes it easier to understand and support (Bottino, 2006). The architecture itself must be easy to maintain, since it will be

constantly changing (Fenz et al., 2008), and must be customized to the specific needs of the organization (Soomro et al., 2016). An architecture also allows organizations to quickly assess the impact of any new vulnerability discovered within the architecture (Fenz et al., 2008), and helps organizations provide business continuity (Soomro et al., 2016).

The design of Enterprise Information Security Architectures usually starts with the business assets and processes. This is the foundation on which the rest of the architectural layers are built, as this ultimately identifies which security measures need to be implemented (Andrews et al., 2014; Goudalo and Seret, 2009; Mukundan and Sai, 2014). This is regarded as the 'top-down' approach, and must consider the full life-cycle of the organization's information, including third party processing and sharing, and cater for the interfaces that these processes require (B Farroha and Farroha, 2011; Ohki et al., 2009; Soomro et al., 2016). In this way, the expenditure on security solutions is easier to justify.

An architecture can make it easier for less experienced personnel to follow good security practices, which can be especially beneficial for small to medium enterprises (AlHogail and Berri, 2012). However, most organizations have still not adopted an enterprise information security architecture (Iguer et al., 2014).

Differences between Public & Private Sectors

Our analysis has shown that there are some clear differences in the security challenges faced by the public and private sectors.

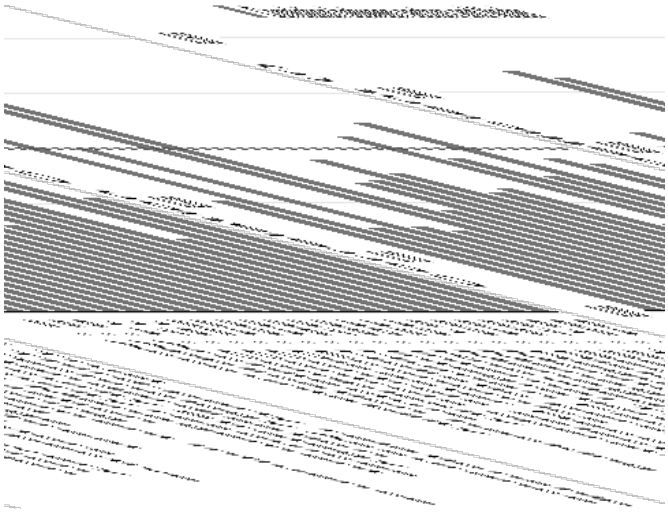

Figure 9 - Nodes that are associated with differences between public and private sectors. The r=0.3 threshold for significant correlations is denoted by a dotted line.

Security challenges for the public sector

Figure 9 shows that **economic** pressure in the public sector is one of the strongest differences between the public and private sectors (r=0.43), and this causes a drain of experienced security professionals towards the private sector (Choo, 2011). These financial constraints can also directly affect disaster recovery (r=0.44), because there are limited resources available to manage the security strategy and respond to incidents (Luethi and Knolmayer, 2009). In addition, outsourcing in the public sector may have caused some loss of control of information assets (Choo, 2011), making **recovery** times for those assets uncertain.

Regulation is another key differentiating factor for this sector, where public sector organizations can be forced to use specific third parties, or bespoke IT solutions (Luethi and Knolmayer, 2009). It seems likely that public sector organizations are more inclined to outsource some of their security requirements to meet imposed **regulations** in the most cost effective way. However, outsourcing to commercial enterprises could increase the risks for a public sector organization, as there is then greater exposure to private sector threats (e.g.

application hacking). Despite any original claims by service providers, profits can quickly influence their priorities, and take away the focus from the security needs of their existing customers.

Regulations also impose greater levels of transparency on public sector organizations, such as disclosing details of their data breaches. These differences can cause public sector organizations to shift their **strategies** and focus their limited resources into areas of security compliance, and this may not address their highest risks in the longer term. For example, controlling information assets in outsourcing contracts maybe be preferable to implementing a complex technical measure that has been imposed.

Public demands to use information in more innovative ways offered by new technology could further increase the risks for public sector organizations (Birman, 2006), outweighing internal warnings about the organization's technical or management ability to keep information protected.

Security challenges for the private sector

There is usually greater **expenditure** on IT in the private sector, where this sector attracts some of the best minds in information security, as the career path and salaries offered exceed those in the public sector (Choo, 2011; Luethi and Knolmayer, 2009). However, even commercial organizations can suffer from a lack of coordinated security **strategy**, which can also impact **disaster recovery** in a similar way to the public sector (Li and Hongyan, 2010).

Application hacking attacks seem to be the largest concern in the private sector (Duncan and Whittington, 2015; Guha and Kandula, 2012). One of the most targeted industries is banking and finance, due to the financial rewards, but there is also concern that parts of the national infrastructure are now at increasing risk from cyber-attack (Choo, 2011). Some commercial

organizations have placed profit ahead of their customer's privacy (Alumark et al., 2015), leading to the misuse of personal information for financial gain.

Discussion

The novelty of this paper is that it both confirms the value of an EISA and summarizes the key factors that must be considered for any EA approach to be successful.

We illustrate this by referencing the original research questions that we gave in the 'Introduction', and highlighting the contributions that this paper is making to the advancement of information security strategies:

(RQ1) To what extent do the root causes of information security incidents relate to potential failings in how an enterprise has implemented its information security programs?

a. **Business and economics can drive security strategies based on flawed risk assessments.** Risk management is complex and it is not acceptable to produce a single risk assessment for information security that simply summarizes risks from high to low. The security risk assessment must be assimilated with departmental risk assessments and describe risks in business terms, based on an accurate assessment against the corporate risk appetite. Unless information security is fully integrated with the business decision-making processes, the business will drive the security strategy without the necessary rigor.

b. **Organizations have to be adaptable and flexible; so security strategies must be too.** Security strategies must integrate with the business so that the most effective security controls are selected, and

their performance regularly assessed to support continuous alignment. As the business changes, so the security strategy must change with it.

c. **Information security is a process, not a product, and cannot be bought. There must be involvement from non-IT and non-security people in its design and maintenance.** The importance of wider management influence on the effectiveness of the security culture of the organization cannot be understated. Monitoring and reacting to security issues are critical to maintaining an effective EISA.

(RQ2) To what extent has enterprise architecture already been seen as a potential solution to make information security more effective?

a. **When implementing information security, it is necessary to account for how an organization functions - it is imperative to maintain the organizational context.** Effective information security requires an holistic view of all the whole company: its goals, processes, information flows, technology, people and partners. EA provides this, by ensuring that technology is built on a sound architecture, where increasing complexity can be managed. We have identified 8 key factors that must work seamlessly together to deliver an effective EISA. This will keep the security strategy focused on agility to meet the demands of the business and identify the presence and impact of new risks.

b. **Separate business functions represent distinct information and must be considered by security strategies.** Information security requires very precise control of corporate assets at all times, wherever and however they are processed and stored. Security risks assessments that

do not consider all copies of information assets are flawed and security policy that conflicts with business processes is destined to fail.

c. **Architectural approaches show promising benefits but are difficult to implement and maintain.** An effective EISA ensures that security is engineered into every aspect of information systems design and makes the technical architecture easier to maintain. It helps to accurately assess information security risks, and respond effectively to security incidents. However, there are clear barriers to its adoption, and we discuss these in our conclusion.

(RQ3) Are there any fundamental differences between the public and private sectors that need to be taken into consideration when embarking on an EA approach to information security?

a. **Regulation can have positive and negative effects on information security.** Regulation helps to make security issues more transparent, but over-regulation can actually increase risks, by forcing organizations to adopt information solutions that may not be best suited their needs. An EISA should still help ensure that these risks are appropriately managed.

b. **Economic factors can harm public sector organizations' recovery from security incidents.** Outsourcing can often be seen as a solution to reducing costs, but this can sometimes be undertaken without due diligence, leading to an unknown change in security risks. An effective EISA should uncover the risks and ensure that they are addressed before the organization makes key decisions about the management of its information.

It is important that the information security strategy complements any existing EA, but it should drive forward its own requirements for the EISA. It should not simply play a 'bit part' of existing EA, as this will not meet the dynamic needs of an effective information security strategy. Our paper is novel in that it has identified 8 domains that are critical to an effective EISA, and has described how these domains need to constantly work together to deliver an effective information security strategy. This paper directly benefits EIS by suggesting how to improve the security context for enterprise architecture design and modelling. It provides a pathway for organizations to effectively improve information security whilst increasing agility and reducing complexity, by proposing a robust foundation for the delivery of a high quality information system that is fully integrated with the enterprise and its business processes. But it can equally apply to any organization that is simply reviewing its information security strategy.

In summary, any successful EISA solution should fulfill the following requirements:

1. involve all business departments in the design of the EISA;
    a. Understand their goals and their information flows;
2. consider all 8 domains described in this paper for all departments, and focus particularly on the areas showing strong correlation, e.g.
    a. How risk management tools need to be aligned;
    b. how technology impacts business processes; and,
    c. how local management is key to delivering security governance;
3. involve the management of these departments in the continuous review and maintenance of the EISA.

Conclusion

Our literature review identified limited direct references to the establishment of a specific EISA. Where EA was described, it was positively in favor of an architectural approach for implementing successful information security practices. Most references to architecture were indirect, in that the literature referenced typical architectural facets as being beneficial to information security.

We studied the root causes of information security failures as part of a systematic literature review. In our quantitative analysis of the causes of IT security failures and successes, we identified 65 elements and their inter-dependencies that influence the success of IT Security programs. We grouped these into eight overarching domains: Business Process; Enterprise Architecture; External Factors; Human Factors; Information Assets; Management Influence; Security Governance; and, Technology Infrastructure.

This research has also shown that there are some differences between the public and private sectors but that these should not present any fundamental changes to how an EISA is implemented, as long as further research affords sufficient consideration to economic constraints and the needs of collaboration.

This paper has emphasized how important it is to develop the ability to uncover hidden security risks and address them as they arise, rather than embark on the relentless pursuit of an ideal state of security optimization, which could become disconnected from real residual security risks being faced by the organization. However, we have also identified some barriers to the adoption of an EA approach. To overcome the barriers, we recommend that further research is undertaken to identify how organizations can adopt the most essential elements of an EA for the benefit of information security programs, and do so using the least resource. A possible solution to this may be to apply a lean and dynamic approach (such as Kanban, the Deming Cycle, or Agile Principles).

Alexander Pope, an 18th-century English poet who gave inspiration for this article's title, is thought to have said knowingly: "Here am I, dying of a hundred good symptoms" when his physician made positive comments about his vital signs on the day that he died. Likewise, the performance of information security must be measured accurately by continuous attention to the whole, and must not be misled by what is commonly referred to as 'vanity metrics'.

Acknowledgements

The authors would like to express their gratitude to the anonymous reviewers for their constructive feedback and helpful advice during the writing of this paper.

References

Adat, Vipindev, and B. B. Gupta. "Security in Internet of Things: Issues, Challenges, Taxonomy, and Architecture." Telecommunication Systems 67, no. 3 (March 2018): 423–41.

Ahmad, Atif, A. B. Ruighaver, And W. T. Teo. "An Information-Centric Approach to Data Security in Organizations." In TENCON 2005 2005 IEEE Region 10. IEEE, 2005.

Oliveira Albuquerque, Robson De, Luis Villalba, Ana Orozco, Fábio Buiati, And Tai-Hoon Kim. "A Layered Trust Information Security Architecture." Sensors 14, no. 12 (December 1, 2014): 22754–72. doi:10.3390/s141222754.

Alhogail, Areej, And Jawad Berri. "Enhancing It Security in Organizations through Knowledge Management." In Information Technology and E-Services (ICITeS), 2012 International Conference on, 1–6. IEEE, 2012.

Alumark A., Hatanaka N., Uchida O., Uchida O. And Ikeda Y. "Identifying the Organizational Factors of Information Security Incidents." 2015 Second International Conference on Computing Technology and Information Management (ICCTIM 2015): Johor, Malaysia, 21 - 23 April 2015. Piscataway, NJ: IEEE, 2015.

Andrews, C., C. Monk, And R. Johnston. "Integrated Architecture Framework and Security Risk Management for Complex Systems." In System Safety and Cyber Security (2014), 9th IET International Conference on, 1–7. IET, 2014.

Asuero, A. G., A. Sayago, And A. G. González. “The Correlation Coefficient: An Overview.” Critical Reviews in Analytical Chemistry 36, no. 1 (January 2006): 41–59. doi:10.1080/10408340500526766.

Atay, Serap, And Marcelo Masera. “Challenges for the Security Analysis of Next Generation Networks.” Information Security Technical Report 16, no. 1 (2011): 3–11.

Atighetchi, Michael, Paul Rubel, Partha Pal, Jennifer Chong, And Lyle Sudin. “Networking Aspects in the DPASA Survivability Architecture: An Experience Report.” In Network Computing and Applications, Fourth IEEE International Symposium on, 219–222. IEEE, 2005.

Atkinson, Colin, Christian Cuske, And Tilo Dickopp. “Concepts for an Ontology-Centric Technology Risk Management Architecture in the Banking Industry.” In Enterprise Distributed Object Computing Conference Workshops, 2006. EDOCW’06. 10th IEEE International, 21–21. IEEE, 2006.

Azmi, Abdul Ghani, Ida Madieha, Sonny Zulhuda, And Sigit Puspito Wigati Jarot. “Data Breach on the Critical Information Infrastructures: Lessons from the Wikileaks.” In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, 306–311. IEEE, 2012.

Farroha, Bassam S., And Deborah L. Farroha. “7.6. 3 Architecting a Secure Enterprise Data Sharing Environment to the Edge.” In INCOSE International Symposium, 21:984–989. Wiley Online Library, 2011.

Bahmani, Faezeh, Marzieh Shariati, And Fereidoon Shams. “A Survey of Interoperability in Enterprise Information Security Architecture Frameworks.” In Information Science and Engineering (ICISE), 2010 2nd International Conference on, 1794–1797. IEEE, 2010.

Baskerville, R., 2004. Agile Security for Information Warfare: A Call for Research. AIS Electronic Library ECIS 2004 Proceedings.

Birman, Ken. “The Untrustworthy Web Services Revolution.” Computer 39, no. 2 (2006): 98–100.

Bottino, Louis J. “Security Measures in a Secure Computer Communications Architecture.” In 25th Digital Avionics Systems Conference, 2006 IEEE/AIAA, 1–18. IEEE, 2006.

Braun, V. And Clarke, V., 2006. Using thematic analysis in psychology. Qualitative research in psychology, 3(2), pp.77-101.

Brunette Jr, Glenn M., And Christoph L. Schuba. “Toward Systemically Secure IT Architectures.” In Enabling Technologies: Infrastructure for Collaborative Enterprise, 2005. 14th IEEE International Workshops on, 8–15. IEEE, 2005.

Chen, Ada Hui-Chuan, Huei-Chung Chu, And Sou-Chein Wu. “Against the Breaches: Data Loss Prevention for Online Travelling Services.” In Information Security and Intelligence Control (ISIC), 2012 International Conference on, 282–285. IEEE, 2012.

Cholez, Hervé, And Christophe Feltus. “Towards an Innovative Systemic Approach of Risk Management,” 61–64. ACM Press, 2014. doi:10.1145/2659651.2659734.

Choo, Kim-Kwang Raymond. “The Cyber Threat Landscape: Challenges and Future Research Directions.” Computers & Security 30, no. 8 (November 2011): 719–31. doi:10.1016/j.cose.2011.08.004.

Collmann, J., And T. Cooper. “Breaching the Security of the Kaiser Permanente Internet Patient Portal: The Organizational Foundations of Information Security.” Journal of the American Medical Informatics Association 14, no. 2 (March 1, 2007): 239–43. doi:10.1197/jamia.M2195.

Cooper, Deborah L. “Data Security: Data Breaches,” 1–3. Proceedings of the 2015 Information Security Curriculum Development Conference, 2015. doi:10.1145/2885990.2886003.

Duncan, Bob, And Mark Whittington. “Information Security in the Cloud: Should We Be Using a Different Approach?,” 523–28. IEEE, 2015. doi:10.1109/CloudCom.2015.92.

Dzazali, Suhazimah, Ainin Sulaiman, And Ali Hussein Zolait. “Information Security Landscape and Maturity Level: Case Study of Malaysian Public Service (MPS) Organizations.” Government Information Quarterly 26, no. 4 (October 2009): 584–93. doi:10.1016/j.giq.2009.04.004.

Farkas, Csilla, And Michael N. Huhns. “Securing Enterprise Applications: Service-Oriented Security (SOS).” In E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services, 2008 10th IEEE Conference on, 428–431. IEEE, 2008.

Fenz, Stefan, Andreas Ekelhart, And Edgar Weippl. “Fortification of IT Security by Automatic Security Advisory Processing,” 575–82. IEEE, 2008. doi:10.1109/AINA.2008.69.

“Gartner Enterprise Architecture Process: Evolution 2005 - GartnerEA.pdf.” Accessed January 27, 2017. http://www.idi.ntnu.no/emner/tdt4175/pdfs/GartnerEA.pdf.

Goudalo, Wilson, And Dominique Seret. “The Process of Engineering of Security of Information Systems (ESIS): The Formalism of Business Processes,” 105–13. IEEE, 2009. doi:10.1109/SECURWARE.2009.24.

Guha, Saikat, And Srikanth Kandula. “Act for Affordable Data Care.” In Proceedings of the 11th ACM Workshop on Hot Topics in Networks, 103–108. ACM, 2012.

Gupta, B. B., Shashank Gupta, and Pooja Chaudhary. “Enhancing the Browser-Side Context-Aware Sanitization of Suspicious HTML5 Code for Halting the DOM-Based XSS Vulnerabilities in Cloud.” *International Journal of Cloud Applications and Computing (IJCAC)* 7, no. 1 (January 1, 2017): 1–31. https://doi.org/10.4018/IJCAC.2017010101.

Gupta, Brij B. *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives*. CRC Press, 2018.

Gupta, Brij, Dharma P. Agrawal, and Shingo Yamaguchi, eds. *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security:* Advances in Information Security, Privacy, and Ethics. IGI Global, 2016. https://doi.org/10.4018/978-1-5225-0105-3.

Herath, Tejaswini, And H. Raghav Rao. “Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations.” European Journal of Information Systems 18, no. 2 (2009): 106–125.

Iguer, Hajar, Hicham Medromi, Adil Sayouti, Soukaina Elhasnaoui, And Sophia Faris. “The Impact of Cyber Security Issues on Businesses and Governments: A Framework for Implementing a Cyber Security Plan,” 316–21. IEEE, 2014. doi:10.1109/FiCloud.2014.56.

Jafarov, Zafar. “Architecture of an Intelligent System for Information Security Management.” In Application of Information and Communication Technologies (AICT), 2013 7th International Conference on, 1–3. IEEE, 2013.

Jeong, Kimoon, Junhyung Park, Minsoo Kim, And Bongnam Noh. “A Security Coordination Model for an Inter-Organizational Information Incidents Response Supporting Forensic Process,” 143–48. IEEE, 2008. doi:10.1109/NCM.2008.126.

Johnston, Allen C., Et Al. "Dispositional and situational factors: influences on information security policy violations." European Journal of Information Systems 25.3 (2016): 231-251.

Kaisler, Stephen H., Frank Armour, And Michael Valivullah. “Enterprise Architecting: Critical Problems.” In System Sciences, 2005. HICSS’05. Proceedings of the 38th Annual Hawaii International Conference on, 224b–224b. IEEE, 2005.

Kerschbaum, Florian. “Building A Privacy-Preserving Benchmarking Enterprise System.” Enterprise Information Systems, n.d., 15.

Khidzir, Nik Zulkarnaen, Azlinah Mohamed, And Noor Habibah Arshad. “Information Security Risk Factors: Critical Threats Vulnerabilities in ICT Outsourcing.” In Information Retrieval & Knowledge Management, (CAMP), 2010 International Conference on, 194–199. IEEE, 2010.

B. Kitchenham And S. Charters, “Guidelines for Performing Systematic Literature Reviews in Software Engineering (Version 2.3),” Technical Report EBSE-2007-01, Keele Univ., EBSE, 2007.

Lalanne, Vincent, Manuel Munier, And Alban Gabillon. “Information Security Risk Management in a World of Services,” 586–93. IEEE, 2013. doi:10.1109/SocialCom.2013.88.

Lechler, Thomas, Susanne Wetzel, And Richard Jankowski. “Identifying and Evaluating the Threat of Transitive Information Leakage in Healthcare Systems.” In System Sciences (HICSS), 2011 44th Hawaii International Conference on, 1–10. IEEE, 2011.

Li, Jianzhong, Chuying Yu, B. B. Gupta, and Xuechang Ren. “Color Image Watermarking Scheme Based on Quaternion Hadamard Transform and Schur Decomposition.” *Multimedia Tools and Applications* 77, no. 4 (February 1, 2018): 4545–61. https://doi.org/10.1007/s11042-017-4452-0.

Li, Xu, And Liu Hongyan. “Proposal for Information Security Architecture Based on a Company.” In Communication Systems, Networks and Applications (ICCSNA), 2010 Second International Conference on, 1:17–20. IEEE, 2010.

Luethi, Martin, And Gerhard F. Knolmayer. “Security in Health Information Systems: An Exploratory Comparison of US and Swiss Hospitals.” In System Sciences, 2009. HICSS’09. 42nd Hawaii International Conference on, 1–10. IEEE, 2009.

Malcolmson, Jo. “What Is Security Culture? Does It Differ in Content from General Organizational Culture?” In Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on, 361–366. IEEE, 2009.

Mao, Handong, Aihua Bao, And Weiming Zhang. “A Logic-Reasoning Approach to Network Security Analysis,” 543–46. IEEE, 2007. doi:10.1109/SKG.2007.156.

Martin, Nigel, And John Rice. “Cybercrime: Understanding and Addressing the Concerns of Stakeholders.” Computers & Security 30, no. 8 (November 2011): 803–14. doi:10.1016/j.cose.2011.07.003.

Masood, Adnan. “Cyber Security for Service Oriented Architectures in a Web 2.0 World: An Overview of SOA Vulnerabilities in Financial Services.” In Technologies for Homeland Security (HST), 2013 IEEE International Conference on, 1–6. IEEE, 2013.

Michelberger, Pál Jr., And Lábodi, Csaba. “After Information Security – Before a Paradigm Change (A Complex Enterprise Security Model)”. Acta Polytechnica Hungarica Vol. 9, No. 4, 2012.

Mukundan, N. R., And L. Prakash Sai. “Perceived Information Security of Internal Users in Indian IT Services Industry.” Information Technology and Management 15, no. 1 (March 2014): 1–8. doi:10.1007/s10799-013-0156-y.

Neuendorf, Kimberly A. The Content Analysis Guidebook. Thousand Oaks, Calif: Sage Publications, 2002.

Ohki, Eijiroh, Yonosuke Harada, Shuji Kawaguchi, Tetsuo Shiozaki, And Tetsuyuki Kagaya. “Information Security Governance Framework.” In Proceedings of the First ACM Workshop on Information Security Governance, 1–6. ACM, 2009.

Onabajo, Prince, Pavol Zavarsky, Dale Lindskog, And Ron Ruhl. “The Study of Civil Litigation in Data Storage Environment.” In Internet Security (WorldCIS), 2012 World Congress on, 224–230. IEEE, 2012.

Park, Sangseo, Atif Ahmad, And Anthonie B. Ruighaver. “Factors Influencing the Implementation of Information Systems Security Strategies in Organizations.” In Information Science and Applications (ICISA), 2010 International Conference on, 1–6. IEEE, 2010.

Pendleton, Marcus, Richard Garcia-Lebron, Jin-Hee Cho, and Shouhuai Xu. “A Survey on Systems Security Metrics.” ACM Computing Surveys 49, no. 4 (December 20, 2016): 1–35.

Polstra Iii, Robert M. “A Case Study on How to Manage the Theft of Information.” In Proceedings of the 2nd Annual Conference on Information Security Curriculum Development, 135–138. ACM, 2005.

NVivo qualitative data analysis Software; QSR International Pty Ltd. Version 10, 2014.

Razavi, Sanaz Hafezian, And Olivia Das. “Evaluating Security Measures of a Layered System.” In Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto International Conference, 296–301. IEEE, 2009.

Renato, Cumbal, And Narvaez Maria. “Technologies’ Application, Rules, and Challenges of Information Security on Information and Communication Technologies,” 380–86. IEEE, 2015. doi:10.1109/APCASE.2015.74.

Sadki, Souad, And Hanan El Bakkali. “Towards Controlled-Privacy in E-Health: A Comparative Study.” In Multimedia Computing and Systems (ICMCS), 2014 International Conference on, 674–679. IEEE, 2014.

Samaras, Vasileios, Semir Daskapan, Rabiah Ahmad, And Samit K. Ray. “An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD.” In Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian, 129–134. IEEE, 2014.

Sen, Ravi, And Sharad Borle. “Estimating the Contextual Risk of Data Breach: An Empirical Approach.” Journal of Management Information Systems 32, no. 2 (April 3, 2015): 314–41. doi:10.1080/07421222.2015.1063315.

H. Shah And M.E. Kourdi, "Frameworks for Enterprise Architecture," IT Professionals, vol. 9, no. 5, 2007, pp. 36-41.

Shaikh, Riaz A., Saeed Rajput, S. M. H. Zaidi, And Kashif Sharif. “Comparative Analysis and Design Philosophy of next Generation Unified Enterprise Application Security.” In Emerging Technologies, 2005. Proceedings of the IEEE Symposium on, 517–524. IEEE, 2005.

Shariati, Marzieh, Faezeh Bahmani, And Fereidoon Shams. “Enterprise Information Security, a Review of Architectures and Frameworks from Interoperability Perspective.” Procedia Computer Science 3 (2011): 537–43. doi:10.1016/j.procs.2010.12.089.

Sherif, Emad, Steven Furnell, And Nathan Clarke. “Awareness, Behaviour and Culture: The ABC in Cultivating Security Compliance.” In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 90–94. IEEE, 2015.

Shropshire, Jordan. “A Canonical Analysis of Intentional Information Security Breaches by Insiders.” Information Management & Computer Security 17, no. 4 (October 9, 2009): 296–310. doi:10.1108/09685220910993962.

Singh, Anand, And David Lilja. “Improving Risk Assessment Methodology: A Statistical Design of Experiments Approach.” In Proceedings of the 2nd International Conference on Security of Information and Networks, 21–29. ACM, 2009.

Sommestad, Teodor, Mathias Ekstedt, And Peter Johnson. “Cyber Security Risks Assessment with Bayesian Defense Graphs and Architectural Models.” In System Sciences, 2009. HICSS’09. 42nd Hawaii International Conference on, 1–10. IEEE, 2009.

Soomro, Zahoor Ahmed, Mahmood Hussain Shah, And Javed Ahmed. “Information Security Management Needs More Holistic Approach: A Literature Review.” International Journal of Information Management 36, no. 2 (April 2016): 215–25. doi:10.1016/j.ijinfomgt.2015.11.009.

Stango, Antonietta, Neeli R. Prasad, And Dimitris M. Kyriazanos. “A Threat Analysis Methodology for Security Evaluation and Enhancement Planning,” 262–67. IEEE, 2009. doi:10.1109/SECURWARE.2009.47.

Stergiou, Christos, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. “Secure Integration of IoT and Cloud Computing.” Future Generation Computer Systems 78 (January 2018): 964–75.

Sun, Jianguang, And Yan Chen. “Intelligent Enterprise Information Security Architecture Based on Service Oriented Architecture,” 196–200. IEEE, 2008. doi:10.1109/FITME.2008.30.

Tahajod, Maryam, Azadeh Iranmehr, And Mohammad Reza Darajeh. “A Roadmap to Develop Enterprise Security Architecture.” In Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for, 1–5. IEEE, 2009.

Tanaka, Hideyuki. “Quantitative Analysis of Information Security Interdependency between Industrial Sectors.” In Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement, 574–583. IEEE Computer Society, 2009.

Group, The Open. TOGAF Version 9.1. 10th New edition. Zaltbommel: van Haren Publishing, 2011.

Tsaih, Rua-Huan, Wan-Ying Lin, And Ada Chen. “Safeguard Gaps and Their Managerial Issues.” Industrial Management & Data Systems 108, no. 5 (May 23, 2008): 669–76. doi:10.1108/02635570810876787.

Tsohou, A., Karyda, M., Kokolakis, S. And Kiountouzis, E., 2015. Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems, 24(1), pp.38-58.

Vallerand, Jonathan, James Lapalme, and Alexandre Moïse. “Analysing Enterprise Architecture Maturity Models: A Learning Perspective.” Enterprise Information Systems 11, no. 6 (July 3, 2017): 859–83.

Waly, Nesren, Rana Tassabehji, And Mumtaz Kamala. “Improving Organizational Information Security Management: The Impact of Training and Awareness,” 1270–75. IEEE, 2012. doi:10.1109/HPCC.2012.187.

Wang, Hui, Heli Xu, Bibo Lu, And Zihao Shen. “Research on Security Architecture for Defending Insider Threat,” 30–33. IEEE, 2009. doi:10.1109/IAS.2009.53.

Whitman, Michael E., And Herbert J. Mattord. Principles of Information Security. 4th ed. Boston, MA: Course Technology, 2012.

Xiong, Ping, Lefeng Zhang, and Tianqing Zhu. “Reward-Based Spatial Crowdsourcing with Differential Privacy Preservation.” Enterprise Information Systems 11, no. 10 (November 26, 2017): 1500–1517.

Zhang, Xuan, Nattapong Wuwong, Hao Li, And Xuejie Zhang. “Information Security Risk Management Framework for the Cloud Computing Environments,” 1328–34. IEEE, 2010. doi:10.1109/CIT.2010.501.

Zhang, Zhenjiang, Xiaoni Wang, Lorna Uden, Peng Zhang, and Yingsi Zhao. “E-DMDAV: A New Privacy Preserving Algorithm for Wearable Enterprise Information Systems.” *Enterprise Information Systems* 12, no. 4 (April 21, 2018): 492–504. https://doi.org/10.1080/17517575.2017.1308559.

Zhao, Gang. “Holistic Framework of Security Management for Cloud Service Providers.” In Industrial Informatics (INDIN), 2012 10th IEEE International Conference on, 852–856. IEEE, 2012.

Appendix

Appendix A – List of nodes

Accidental	Controls selection	Integration	Risk management
Accountability	Least privilege	Internal threat	Security resources
Accuracy	Culture	Interoperability	Security strategy
Agility	Dependency	Knowledge	Social environment
Application hacking	Disaster recovery	Managed	Standardization
Architecture	Documentation	Management assurance	Supervision
Asset management	Economics	Management influence	Systems thinking
Automation	Enterprise structure	Monitoring	Systems perspective
Business continuity	External to secure network	Multiple vulnerabilities	Technology assurance
Business process	Flexibility	New technology	Third-party relationship
Business-driven	Scalability	Non-digital	Timescales
Communication	Fragmentation	Openness	Trust
Compartmentalization	Framework	Performance degradation	Uncertainty
Complexity	Governance	Persuasion	Predictability
Configuration	Holistic perspective	Redundancy	
Continuous improvement	Human factors	Regulation	
Controls operation	Information sharing	Reliability	

Table 9 – List of nodes that capture root causes of success or failure of information security