Frameworks of Governance and Cybersecurity Management

James J. Fisher, Cybersecurity Leader
Inspire Secure Enablement of Business

Abstract

A critical analysis of concepts, theories, and literature concerning the impact of frameworks on governance and cybersecurity management. This will include trends, challenges, and issues related to the implementation of governance and cybersecurity management within the modern business landscape. An assessment of solutions and limitations will include impacts from frameworks for implementing governance and cybersecurity management, with a discussion on the TJX Companies, Inc. cybersecurity breach.

Keywords: frameworks, best practices, cybersecurity, information security, governance, architecture, management, leadership, SABSA, ISO/IEC 27000, PCI-DSS, TJX

Note: This is not a peer-reviewed research paper. Do not use as a primary or secondary source within a thesis, dissertation, or research paper. If a reasonable perspective for research is found and a viable research perspective is being considered, please reach out to the author: jjfisher@jamesjfisher.org.

Updated: July 3, 2025

Introduction

Governance and cybersecurity management are critical organizational constraints in today's business environment. Protecting information resources is a crucial factor in achieving organizational success, particularly as threats continue to evolve. Yet, many organizations struggle to secure these resources due to a narrow focus on cybersecurity operationalization (Burkett, 2012). The boundary between business, IT, and cybersecurity has dissolved, and organizations can no longer focus solely on compliance at minimal cybersecurity levels (Burkett, 2012). Such a checkbox mentality results in reactive responses to cybersecurity incidents, more after-action investigations, and breaches (Burkett, 2012). Modern businesses must adopt holistic, proactive approaches that address every layer of the enterprise, blending both business and risk considerations (Burkett, 2012). Solutions to business problems should be industry-agnostic across all enterprise layers (Burkett, 2012). Many organizations base their efforts on frameworks, standards, and best practices to guide the deployment of technology, cybersecurity, policies, and processes. Often, organizations try to adopt these frameworks as they are, rather than tailoring them to their specific needs. This approach affects their ability to manage cybersecurity and governance effectively.

Background

Organizations that focus on adapting to frameworks instead of adapting frameworks to their organizations will see impacts on governance and cybersecurity management. Organizations should focus their efforts on supporting and enabling the business, rather than reacting to a need without understanding the organization, its requirements, and the long-term impacts presented by frameworks that may not be appropriate for the organization (Cherdantseva, Rana, & Hilton, 2011). Likewise, governance and cybersecurity management must be driven by business needs, risk considerations, and prioritization of IT and cybersecurity to deliver value to organizations (Ali & Soomro, 2014; Burkett, 2012; Cherdantseva et al., 2011; Elkhannoubi & Belaissaoui, 2016; Weill & Ross, 2008). To accomplish this direction, both governance and cybersecurity management will need to meet specific goals.

Goals

Daily, organizations are exposed to cybersecurity threats both internally and externally. Organizations must prioritize the safety of their information resources; however, current cybersecurity technologies and methods may not provide an acceptable level of cybersecurity based on risk. (Elkhannoubi & Belaissaoui, 2016). Organizations need to invest in effective cybersecurity management to meet the goals of preserving integrity, availability, and confidentiality, thereby prioritizing the safety of information resources (Elkhannoubi & Belaissaoui, 2016). Cybersecurity prioritization of information resources is an effort to protect an organization from intentional and unintentional threats and risks (Elkhannoubi & Belaissaoui, 2016). Cybersecurity management presents a combination of methods, skill sets, and rules to improve cybersecurity, requiring a consistent approach that encompasses legal, technological, managerial, procedural, organizational, and human competence dimensions (Elkhannoubi & Belaissaoui, 2016). Cybersecurity prioritization and efforts to safeguard information resources are also related to IT governance.

Governance has a broad umbrella that focuses on the overall technology delivered throughout an enterprise. Enterprise implementations of governance focus on structures, processes, and communications, requiring them to be designed with clarity and transparency in mind (Weill & Ross, 2008). These structures, ideally, aim to promote specific behaviors within the organization, driving change management across both the business and IT organizations (Weill & Ross, 2008). Ideally, governance involves IT and business leaders in making decisions that align with the organization’s goals, objectives, and needs to achieve a competitive advantage (Weill & Ross, 2008). As a specific set of goals, governance requires involvement from company leadership, with a focus on clarity and transparency across structures,

processes, and communication (Weill & Ross, 2008). Frameworks are necessary for delivering governance and cybersecurity management within an organization.

With organizations facing internal and external threats, frameworks for governance and cybersecurity are essential components of part of enterprise IT service and cybersecurity delivery. Organizations must invest in effective governance and cybersecurity management, prioritizing the cybersecurity of their information resources (Elkhannoubi & Belaissaoui, 2016; Weill & Ross, 2008). Both governance and cybersecurity management present as a combination of skill sets with a focus on structures, processes, and communication (Elkhannoubi & Belaissaoui, 2016; Weill & Ross, 2008). Both governance and cybersecurity management require a consistent approach, encompassing legal, technological, managerial, procedural, organizational, and human competence dimensions within clear and transparent designs (Elkhannoubi & Belaissaoui, 2016; Weill & Ross, 2008). Both governance and cybersecurity management aim to promote desired behavior while incorporating input from IT and business leaders to inform decisions that align with business goals, objectives, and the organization's needs for competitive advantage (Weill & Ross, 2008). Within an organization, this will take shape by utilizing both governance and cybersecurity frameworks.

Frameworks

Frameworks are generic constructs that typically include standards, best practices, methodologies, and operational practices, which can be strategic, tactical, or operational, or a combination thereof. Frameworks, standards, and best practices are generally applicable, although some are specific to enterprise architecture, cybersecurity architecture, or governance (Burkett, 2012; Cherdantseva et al., 2011; Weill & Ross, 2008). Organizations must have frameworks, standards, and best practices to drive overall governance and cybersecurity management. Several frameworks currently exist, including ITIL, COBIT, and the ISO/IEC 27000 series, which SABSA and the PCI-DSS support. Not all are created equally or have the same focus.

Information Technology Information Library (ITIL)

The Central Computer and Telecommunications Agency (CCTA) developed ITIL and was merged with the Office of Government Commerce (OGC) of the United Kingdom in the eighties (Ahmad, Amer, Qutaifan, & Alhilali, 2012; Ali & Soomro, 2014). ITIL is a service management standard library that focuses on the IT organization and is considered an IT governance framework focused on information technology system management (ITSM) (Ahmad et al., 2012). This includes an array of standards and best practices that were culled from both private and public sector best practices over a twenty-year timeframe (Ahmad et al., 2012). ITIL, also a quality framework, emphasizes reorganizing the work of staff but not reorganizing the staff, which creates "benefits such as cost savings, risk management, and streamlining IT operations" (Ahmad et al., 2012, p. 554). ITIL has a specific focus on the service management of IT processes and service delivery.

ITIL's focus on service management and service delivery comes from being a collection of best practices for IT services management. This allows ITIL to help organizational awareness of business value within IT services delivered to internal and external stakeholders (Ali & Soomro, 2014). ITIL is centered around key management disciplines with a focus on financial, service level, continuity, configuration, and change management (Ali & Soomro, 2014). Likewise, ITIL is oriented around service desk functions to maintain release, incident, and problem management (Ali & Soomro, 2014). This enables ITIL to empower organizations to enhance their service management while delivering IT services with higher degrees of quality (Ali & Soomro, 2014). ITIL with a focus on service management and delivery is, therefore, less governance-oriented.

ITIL is not entirely focused on governance but on service management. With ITIL focusing on key management disciplines, these concepts overlap with governance and

governance goals (Ali & Soomro, 2014; Weill & Ross, 2008). This overlap is considered within a discussion on quality, cost reduction, risk management, and delivery of business value through strong, clear, and transparent processes (Ali & Soomro, 2014; Weill & Ross, 2008). This is unlike COBIT, which is entirely focused on governance.

Control Objectives for Information and Related Technology (COBIT)

The Information Systems Audit and Control Association (ISACA) developed the Control Objectives for Information and Related Technology (COBIT) as a general, all-purpose information technology governance framework (Ali & Soomro, 2014). COBIT is utilized as an IT governance framework, comprising a series of related IT controls, with auditing in mind (Ali & Soomro, 2014). The focus of COBIT is to enable broader decision-making for IT management, without delving into technical details (Ali & Soomro, 2014). COBIT is a comprehensive framework that focuses on managing IT resources from a process-oriented perspective.

COBIT is a framework of best practices related to IT resource management. This presents best practices within the framework, with an emphasis on resource management, infrastructure, processes, responsibilities, and controls (Ali & Soomro, 2014). COBIT is a comprehensive body of work that encompasses controls, standards, practices, and methodologies, while also being auditable, measurable, and reportable (Ali & Soomro, 2014). COBIT has a maturity model that mirrors other capability maturity models; however, the emphasis is on the maturity of implementing COBIT controls within an IT governance context (Ali & Soomro, 2014). It is generally the first choice in frameworks for IT governance globally, primarily due to its widespread availability through ISACA (Ali & Soomro, 2014). COBIT serves as a driver for governance within an organization, as it addresses the key goals of governance.

COBIT, when applied to governance, addresses many of the goals discussed by Weill and Ross (2008). The extensive body of controls, standards, practices, and methodologies presented by COBIT focuses on structures, processes, communications, responsibility, and accountability, with the requirement that they be designed with clarity and transparency in mind (Ali & Soomro, 2014; Weill & Ross, 2008). Like the structures described by Weill and Ross (2008), the best practices of COBIT attempt to drive desired behavior within the organization while being inclusive of leadership decision-making to meet business goals, objectives, and needs of the organization for competitive advantage (Ali & Soomro, 2014; Weill & Ross, 2008). COBIT is a broad governance framework, less specific to service management than ITIL, and does not address cybersecurity concern, such as those addressed by SABSA.

Sherwood Applied Business Security Architecture (SABSA)

SABSA is a cybersecurity architecture development framework developed by John Sherwood and has been utilized, primarily in Europe, since 2005. SABSA is a business-oriented and risk-driven framework for developing cybersecurity architectures within an organization, with integration capabilities for enterprise architecture frameworks such as the Open Architecture Framework (TOGAF) and the Zachman Framework. (Burkett, 2012). As an architectural framework, SABSA can stand on its own from a cybersecurity perspective.

SABSA provides integrated frameworks, models, methods, and processes that are risk-driven, addressing threats and opportunities with a focus on best practices (Burkett, 2012). The methodology and approach are business-oriented within a “six-layer model covering the four parts of the IT lifecycle: strategy, design, implementation, and management & operations” (Burkett, 2012, p. 48). Cybersecurity solutions are derived from these layers to produce business requirements (Burkett, 2012). This enables cybersecurity professionals to concentrate on business-oriented cybersecurity solutions.

SABSA enables cybersecurity professionals to become providers of cybersecurity solutions, rather than the business operations inhibitors that organizations often perceive them to be (Burkett, 2012). This stems from the adaptability of SABSA to any enterprise, facilitated by its integration within existing enterprise architectures due to its holistic and technology-agnostic

nature (Burkett, 2012). This is achieved through the integration of multiple cybersecurity dimensions across various enterprise layers, aligning with existing enterprise architectures and building on existing strengths while minimizing the introduction of new risks (Burkett, 2012). This essentially means SABSA can integrate with ITIL, COBIT, PCI-DSS, and even the ISO/IEC 27000 series, but is not focused on the same premises. SABSA would utilize other frameworks as inputs to the cybersecurity architecture process, such as the ISO/IEC 27000 series standards, to deliver an internationally oriented cybersecurity architecture.

ISO/IEC 27000 Series

The ISO/IEC 27000 series of standards is published jointly by the International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC) (Cherdantseva et al., 2011) The ISO/IEC 27000 series is reserved for information security specifying requirements for an information security management system (ISMS) (Cherdantseva et al., 2011). The ISO/IEC 27000 series encompasses a broad range of information security-related issues across various dimensions, including risk assessment, management responsibilities, management commitment, resource management, resource provisioning, training, awareness, and competence (Ali & Soomro, 2014; Cherdantseva et al., 2011). The ISO/IEC 27000 series is a globally accepted code of practice.

As an international framework of controls, standards, and best practices, it includes a code of practice for information security management concerning an ISMS (Ali & Soomro, 2014; Cherdantseva et al., 2011). Likewise, the ISO/IEC 27000 also defines information security policy development (ISPD) (Cherdantseva et al., 2011). Literature generally focuses on ISO/IEC 27001 and 27002, which encompass a substantial number of domains for ISMS coverage within an organization (Ali & Soomro, 2014; Cherdantseva et al., 2011). The ISO/IEC 27000 series is a comprehensive framework for the internationalization of information security management, being industry-agnostic.

A key characteristic of the ISO/IEC 27000 series is its industry-agnostic nature. This generally means any organization can adapt the framework to their organization. However, even as a code of practice, the ISO/IEC 27000 series focuses on a single organization within a closed system (Cherdantseva et al., 2011). However, it does address issues of importance across a broad set of domains that are easily identifiable to an organization and can be integrated with SABSA to deliver a cybersecurity architecture for information security management (Ali & Soomro, 2014; Burkett, 2012; Cherdantseva et al., 2011). Although it can be considered a governance framework, it is specific to delivering an information security management system, rather than encompassing all aspects of IT governance. Nevertheless, it can be integrated with ITIL, COBIT, and SABSA.

Payment Card Industry-Data Security Standard (PCI-DSS)

The Payment Card Industry-Data Security Standard (PCI-DSS) was developed jointly by the card brands (American Express, Visa, Master Card, Discover, and JCB) (PCI-SSC, 2016). Major revisions occur on a three-year cycle, while minor versions can be released on an annual basis, typically for clarity (PCI-SSC, 2016). The PCI-DSS is mandated by the card brands for any entity that stores, transmits, or processes credit cards (PCI-SSC, 2016). The PCI-DSS has an extremely narrow focus, protecting only credit card numbers, referred to as primary account numbers (PANs), and the information present on the magnetic stripe of a credit card. The PCI-DSS is a contractually obligated standard and not mandated by regulation.

The PCI-DSS is not a governance framework or technically a security framework. The PCI-DSS, as noted by the PCI-SSC (2016), is only specific to credit card transactions and nothing more. It lacks real teeth and is primarily a compliance effort related to governance and cybersecurity management. It lacks the comprehensive control framework of COBIT or the ISO/IEC 27000 series. Although it can be integrated with SABSA and ITIL, it isn't necessarily congruent with COBIT or ISO/IEC 27000 series.

Evaluation of Developments and Trends

The goal of cybersecurity management is to enable business operations with features and advantages that lead to benefits at each of the varying layers of an enterprise, regardless of the enterprise architecture utilized (Burkett, 2012; Cherdantseva et al., 2011). Cybersecurity architecture must meet unique business needs while providing necessary flexibility for integration with existing enterprise architectures, managing complexity, ensuring architectural governance, providing two-way traceability on key decisions, measuring true organizational value, being risk-driven, and being business-driven (Burkett, 2012; Cherdantseva et al., 2011). Cybersecurity architecture comes into play with the understanding an enterprise cannot protect its information assets without understanding the entirety of its lifecycle (De Oliveira Albuquerque, García Villalba, Sandoval Orozco, Buiati, & Kim, 2014). Cybersecurity countermeasures must provide reasonable levels of assurance within the cybersecurity architecture, where cybersecurity management provides a systematic approach consistently across every layer within the trust model and organization (De Oliveira Albuquerque et al., 2014). Cybersecurity architecture and cybersecurity management are closely tied to IT governance.

Governance with a focus on delivering change within an organization is also concerned with decision-making and accountability. Decision-making encompasses accountability across five key areas, including IT principles, enterprise architecture, IT infrastructure, business needs, and investment prioritization (Weill & Ross, 2009). Much of this is accomplished through roles, committees, teams, and formal processes to reduce costs, increase return on investment, and provide accountability across an organization (Weill & Ross, 2009). This is essentially the same as noted above, with cybersecurity architecture that overlaps with enterprise architecture.

Governance and cybersecurity management overlap. Both governance and cybersecurity management are concerned with decision-making and accountability (Burkett, 2012; Cherdantseva et al., 2011; De Oliveira Albuquerque et al., 2014; Weill & Ross, 2009). Both governance and cybersecurity management have a focus on decision-making and accountability within IT principles, enterprise architecture, IT infrastructure, business needs, and investment prioritization (Burkett, 2012; Cherdantseva et al., 2011; De Oliveira Albuquerque et al., 2014; Weill & Ross, 2009). This is accomplished through roles, committees, teams, and formal process to reduce costs, increase return on investment, and provide accountability across an organization to enable business with features, advantages, and benefits at every layer of an enterprise (Burkett, 2012; Cherdantseva et al., 2011; De Oliveira Albuquerque et al., 2014; Weill & Ross, 2008; Weill & Ross, 2009). Both governance and cybersecurity management strive to meet the unique needs of a business mission by being flexible, integrating with enterprise architectures, managing complexity, and providing architectural governance while being risk-driven and business-oriented (Burkett, 2012; Cherdantseva et al., 2011; De Oliveira Albuquerque et al., 2014; Weill & Ross, 2008; Weill & Ross, 2009). A trend is slowly emerging within the literature.

Considering how literature is now starting to present more integrated conversations, it is not entirely surprising to see this trend presenting itself. The discussions thus far have compared ITIL and COBIT with the ISO/IEC 27000 series, with a particular focus on the intersection between enterprise architecture and cybersecurity architecture. It would seem logical to assume that, over time, more discussions will begin to focus on the convergence of governance and cybersecurity management, considering the current threats consistently posed to organizations and the need for cost-effective IT delivery. Additionally, due to the shared goals of governance and cybersecurity management, convergence is a logical direction, considering the relative compartmentalized mentality that used to be present in IT and cybersecurity discussions.

Analysis of Challenges and Issues

Protecting information resources is a commonality and priority for organizational success, particularly in the evolution of external and internal threats that enterprises are currently struggling to protect against (Burkett, 2012). Although the lines between business, information technology, and cybersecurity have blurred, there are still challenges to address (Burkett, 2012). A compliance check box mentality is hurting organizations because meeting mandated compliance standards at a minimum level of cybersecurity provides no value to the organization and increases potential impacts (Burkett, 2012; Cherdantseva et al., 2011). The forward direction for organizations is the utilization of established, proactive approaches and methodologies to governance and cybersecurity management that are business-oriented, risk-based, and incorporate cybersecurity into technology deployments (Ali & Soomro, 2014; Burkett, 2012; Cherdantseva et al., 2011). Frameworks are at the center of this conversation because ineffectively deploying frameworks has real impacts on an organization.

Frameworks

Organizations are devoting a significant amount of energy to frameworks, standards, and best practices without fully understanding how they align with their organization's objectives. Frameworks, standards, and best practices should serve as a strategic deliverable for governance and cybersecurity management. Organizations need to evaluate and choose one or more to follow, then adapt them to their specific needs (Cherdantseva et al., 2011). Organizations must tune and tweak frameworks, standards, and best practices to align with their operating paradigms within their business context, as changing them later will be costly (Cherdantseva et al., 2011). Frameworks, standards, and best practices must strike a balance between information sharing and protection while adhering to legal and compliance limits (Cherdantseva et al., 2011). Likewise, organizations must be aware that those that develop frameworks, standards, and best practices have no financial culpability or liability when an organization implements them, they fail to provide value, or a breach occurs (Cherdantseva et al., 2011). This will impact governance and cybersecurity management practices within an organization, as it affects senior leadership decision-making. The practices within frameworks, standards, and best practices may not entirely align with the organization's operating model or its industry.

Cybersecurity architecture

Tasks within cybersecurity architecture focus on the design, development, and management of secure systems and applications that incorporate a high degree of complexity (Burkett, 2012; Cherdantseva et al., 2011). Both technical and non-technical disciplines have adopted architecture terminology, which is no different from cybersecurity, where cybersecurity architecture (SABSA) focuses on designing and developing secure systems with high degrees of cybersecurity resiliency (Burkett, 2012; Cherdantseva et al., 2011). Cybersecurity architecture and cybersecurity management are focused on the overall cybersecurity of an enterprise. In this manner, security architecture is a framework (SABSA) for delivering cybersecurity controls and mechanisms across the various layers of an enterprise, applications, and systems to ensure they operate coherently together (Cherdantseva et al., 2011). To accomplish coherent operation, three aspects are required to be met first, the business goals of the enterprise; second, the overall environment the enterprise operates within; and third, the technical capability present within currently evolving information and communications technologies (ICT) (Burkett, 2012; Cherdantseva et al., 2011). This is technology-focused, as is often seen within organizations.

Cyberecurity architecture is mainly utilized from a technical perspective, foregoing business goals and the enterprise environment (Burkett, 2012; Cherdantseva et al., 2011). Business goals and the enterprise environment are crucial and must be considered during the design, development, and maintenance of the cybersecurity architecture (Burkett, 2012; Cherdantseva et al., 2011). The tasks involved with cybersecurity architecture are highly

complex by nature and orders of magnitude more complex within modern technology environments (Burkett, 2012; Cherdantseva et al., 2011). Considering mobile, cloud, and various off-premise services, complexity increases as organizational boundaries become more flexible.

De-perimeterization is a term coined by the Jericho Forum, an international association of organizations focused on secure business (Cherdantseva et al., 2011). The term refers to the transition from a hard boundary to a soft boundary, characterized by the loss of organization perimeters and the need to secure an extended boundary (Cherdantseva et al., 2011). Within this new concept and paradigm, third parties have access to data and services internal to an organization, while the organization may also have access to data and services provided or hosted by other organizations (Cherdantseva et al., 2011). Many enterprises have begun to integrate cloud capabilities for storage, services, applications, and high-throughput computation to reduce costs, gain efficiencies, and increase profits (Cherdantseva et al., 2011). This means closed systems with hard boundaries no longer exist when you also factor in remote users, mobile technologies, and the Internet of Things (Cherdantseva et al., 2011). There is a business opportunity in soft boundaries.

Softened enterprise perimeters create opportunities for enterprises with an open architecture; however, this also creates increased cybersecurity and governance challenges, especially given the level of interconnectivity available (Cherdantseva et al., 2011). Previously utilized methods for maintaining perimeter security are untenable and unsustainable for the long term (Cherdantseva et al., 2011). A cybersecurity management approach must account for an enterprise operating within a soft perimeter, with the ability to secure information both inside and outside the enterprise's perimeter (Cherdantseva et al., 2011). This will require multi-layered cybersecurity controls and countermeasures capable of addressing people, processes, technology, and regulations, and be accounted for in governance decision-making (Cherdantseva et al., 2011). Closed systems in this discussion was the system and application paradigm of organizations.

With closed systems, there is the assumption boundaries are equivalent between the organization and the system (Cherdantseva et al., 2011). Whereas the boundary within a de-perimeterized organization is significantly more complicated based on the inability to define the boundary and scope of the organization's information technology system management (ITSM) and information security management system (ISMS) (Cherdantseva et al., 2011). Within de-perimeterization, the cybersecurity of one organization will depend on the reliability of the cybersecurity of other organizations within the soft perimeter (Cherdantseva et al., 2011). This will require inter-organizational collaboration in the event an organization desires to improve its cybersecurity posture (Cherdantseva et al., 2011). When the cybersecurity architecture is integrated with ISO/IEC 27000, de-perimeterization will need to be addressed due to limitations inherent in the ISO/IEC 27000 series.

ISO/IEC 27000

The ISO/IEC 27000 series was developed when organizations were not significantly affected by the concept of de-perimeterization, and as a framework for information security, it only addresses information security within a single enterprise (Cherdantseva et al., 2011). Within a closed system, the boundaries of ITSM and ISMS are easily visualized as being equal to the boundaries of an organization, and under de-perimeterization, this is not true (Cherdantseva et al., 2011). The ISO/IEC 27000 series of standards defines the boundaries and scope of the ISMS, which is part of the overall management of the system (Cherdantseva et al., 2011). Under de-perimeterization, organizations using the ISO/IEC 27000 series will need to define the scope of the ISMS boundaries by additionally including service providers, vendors, suppliers, partners, collaborators, and customers (Cherdantseva et al., 2011). The ISO/IEC 27000 series does not adequately or comprehensively cover the issues of information security within the concept of de-perimeterization from a managerial, governance and cybersecurity management perspective

(Cherdantseva et al., 2011). This is partly due to the closed system and single-enterprise perspective of the ISO/IEC 27000 series (Cherdantseva et al., 2011). In this case, if the ISO/IEC 27000 series is integrated with the cybersecurity architecture, it will need to be addressed as part of governance (COBIT, ITIL) and cybersecurity management within the cybersecurity architecture (SABSA, PCI-DSS).

ITIL

ITIL has become a global standard in IT service management and governance; however, many organizations that have fully implemented ITIL have concluded that not all ITIL processes are necessary, equally important, or of value, and many agree that ITIL implementation is challenging (Ahmad et al., 2012). ITIL faces implementation challenges mainly because it is not well-documented, providing only general guidance on process implementation (Ahmad et al., 2012). This leaves senior leadership uncertain about which ITIL best practices are most relevant to implement (Ahmad et al., 2012). This leads to the condition that consultants, vendors, and in-depth training are a necessity for an organization to implement ITIL (Ahmad et al., 2012). Another issue is the resistance ITIL garners from organizational personnel due to poor organizational change management (Ahmad et al., 2012). Studies within the literature report that organizations decide against ITIL implementation due to insufficient internal support, often related to poor organizational change management (Ahmad, 2012). This occurs despite the fact that ITIL can provide organizational benefits.

There is little doubt in the literature that ITIL best practices can help organizations or IT departments manage internal change by focusing on preparation, benefits to affected personnel, and user involvement (Ahmad et al., 2012). Implementing ITIL, however, is challenging in part because it provides only general guidance and offers no specific direction on implementation (Ahmad et al., 2012). ITIL has flexibility due to this issue, allowing it to work for a wide variety of organizations across different industries; however, it also introduces challenges, as well as the ability to map ITIL processes to the real world (Ahmad et al., 2012). This presents a condition where ITIL is not always the answer, as many reasons for implementing some or all ITIL processes emerge, and organizations must have clear reasoning to measure success and focus efforts on real business and IT problems (Ahmad et al., 2012). For organizations looking to implement ITIL, it is essential to clearly understand the who, what, why, when, where, and how, as well as how cybersecurity will be addressed.

PCI-DSS

The PCI-DSS faces some challenges and issues that stem from its narrow focus. The standard does not include a conversation about personally identifiable information (PII), electronic protected health information (ePHI), protected health information (PHI), or debit card or automated clearing house (ACH) information (PCI-SSC, 2016). The twelve requirements are prescriptive of only the protection of credit card numbers and information found on a credit card magnetic stripe, which presents a conundrum of its own (PCI-SSC, 2016). How do you protect something that requires the implementation of a prescriptive standard without consideration for any other information asset, or consider privacy or cybersecurity concerns for any other form of data or information? Additionally, how is it that the card brands have not been called out on their conflict of interest? The card brands own and directly benefit from developing, creating, and requiring the PCI-DSS for all organizations downstream from the card brands to be PCI-DSS compliant, except for card processors like First Data and Chase Payment Tech. As a contractual mandate for doing business with card brands, issuing banks, and processors, maintaining compliance is the only current impetus.

The PCI-DSS is only contractually mandated, which currently means that no regulations exist mandating its use. The PCI-DSS is mandated contractually when an organization desires to accept credit cards as a form of payment (PCI-SSC, 2016). The upside of this discussion point is that regulation does, in fact, trump PCI-DSS compliance when a company needs to protect multiple streams of information that have regulatory requirements (PCI-SSC, 2016). This

means that some of the cybersecurity controls companies have implemented are stronger than those present in the PCI-DSS, such as log management, encryption, technology use, technology deployment, access controls, and segmentation and isolation (Berg, Freeman, & Schneider, 2008; PCI-SSC, 2016). The downside is that qualified security assessors (QSA) might not understand the controls and mechanisms they are evaluating. The cybersecurity controls implemented by an organization may be stronger than those within the PCI-DSS. However, if the QSA does not understand this paradigm, remediation may be required under the PCI-DSS, potentially reducing the effectiveness of the stronger controls and mechanisms. This situation could put organizations out of compliance with regulatory mandates in the absence of stronger cybersecurity skill sets to argue the point.

The breach of TJX Companies, Inc. serves as a prime example of why frameworks, standards, and best practice compliance do not lead to secure environments. At the time of the breach, TJX was PCI-DSS compliant; however, it also maintained massive amounts of personally identifiable information (PII) on its clients (Chandrasekhar, 2008; Xu, Grant, Nguyen, & Dai, 2008). During the examination of the organization, it was found that TJX was using the Wired Equivalent Privacy (WEP) protocol, already known to be vulnerable, and was used to breach the organization (Chandrasekhar, 2008; Xu, Grant, Nguyen, & Dai, 2008). WEP is notoriously easy to crack, a fact acknowledged by Berg et al. (2008), Chandrasekhar (2008), and Xu et al. (2008). Although both Berg et al. (2008) and Chandrasekhar (2008) criticize TJX for using WEP in their wireless systems, it was technically permissible under the PCI-DSS. The PCI Security Standards Council (2008) under Requirement 4.1.1 of the PCI-DSS version 1.2.1 clearly states that new implementations of WEP were prohibited after March 31, 2009, and in-place installations of wireless had until June 30, 2010, to migrate to the newer standards under IEEE 802.11i. Although TJX should have attempted to move towards a more secure wireless environment, there was no clear impetus under the PCI-DSS between 2005 and 2007, as it wasn't until the 2008 PCI-DSS standards were removed and their use extended into 2010 (PCI Security Standards Council, 2008). Encryption in transit is not the only encryption issue presented.

Encryption of data at rest is another area of concern. Chandrasekhar (2008) does not delve into relevant specifics, such as the algorithms TJX was utilizing or across which systems, other than those supposedly related to terminals and merchandise returns. Berg et al. (2008) suggest in their article that nothing was encrypted or the encryption keys were stolen. Chandrasekhar (2008) does mention the compromise could have included access to the encryption keys and the tools for decrypting data. Berg et al. (2008) make a significant leap in suggesting that encryption is a be-all and end-all method for keeping people out of data. This isn't entirely true, and the scope of encryption within the PCI-DSS at the time of the breach could have included the use of disk encryption, rather than file or column-level encryption, which is also essentially the same under the current PCI-DSS (PCI-SSC, 2016; PCI-SSC, 2008). Under PCI-DSS version 1.2.1, requirement 3.4.1, it is acceptable to use disk encryption if it is not tied directly to the operating system, and this approach remains essentially the same under the current version of PCI-DSS (PCI-SSC, 2016; PCI-SSC, 2008). This creates a loophole wherein logical access to the data is decrypted for anyone with logical access permissions, without requiring any keys. However, if you were to remove the disk drives, walk off with them, and attempt to read the data later, it would be unintelligible, and keys would be necessary. Chandrasekhar (2008) notes that usernames and passwords of associates were pilfered during the wireless attacks, which suggests the intruders didn't need access to encryption keys if disk encryption was being used over either file or column-level encryption. Even if improper storage were not present, this would still be a problem because the control itself remains weak.

Not to belabor the point, the TJX breach notes the problem of relying on the tenets of a security standard with a narrow focus. Many of the controls present in the PCI-DSS during the time of the TJX breach and in current incarnations of the standard are similar and still provide weak controls that can be circumvented with basic knowledge of how those controls work in relation to access control, log management, encryption, and various internal security processes.

Much of this was laid out in detail by Berg et al. (2008), Chandrasekhar (2008), and Xu et al. (2008) as they decomposed the issues leading up to the breach and how items of the PCI-DSS allowed for the breach to continue. Likewise, each noted aspects of governance that was a failure in aligning the business with sound cybersecurity practices that would have moved the company out of danger instead of blindly moving budgets away from fixes and then reactively allocating those budgets to remediation post incident (Berg et al.,2008; Chandrasekhar, 2008; Xu et al., 2008). Much of the issue presented in the TJX breach stemmed from the reliance on a framework in the absence of sound governance and effective cybersecurity management. Such reliance delayed investment in removing the legacy WEP-based wireless system, which led to reactive remediation and significant penalties from litigation and class-action lawsuits. Likewise, the PCI-SSC was not held accountable for its involvement in allowing WEP deployments within its PCI-DSS-mandated controls, which continued well into 2010, a full three years after the TJX breach.

Assessment of Limitations

IT departments tend to operate in a stand-alone manner. Likewise, cybersecurity departments tend to operate in a stand-alone manner, if they exist. This means IT departments and cybersecurity departments, if not integrated into the larger IT organization, can be considered businesses of their own within the overall business, with a business orientation and a resulting management complexity (Buchwald, Urbach, & Ahlemann, 2014). Governance is a crucial discussion point, as IT encompasses organizational, technical, and cultural influences that require governance to manage these areas while maintaining the business orientation of IT (Buchwald et al., 2014). A portion of the literature within the realm of governance discusses structures, frameworks, and processes; however, there is an apparent lack of a shared understanding, which potentially inhibits research within the field (Buchwald et al., 2014). Likewise, literature discusses cybersecurity management separately from governance.

Governance frameworks, standards, and best practices often focus on discussions related to information technology management. Cybersecurity frameworks, standards, and best practices tend toward a focus on the development and maintenance of information security management systems (De Oliveira Albuquerque et al., 2014). In this manner, cybersecurity needs to support business objectives through minimizing risk and developing trust while also taking an iterative approach to continuous improvement (De Oliveira Albuquerque et al., 2014). Frameworks such as ITIL, COBIT, and ISO/IEC, as well as SABSA, are utilized in technology governance to reduce costs, increase productivity, and enhance cybersecurity through organization and methodologies (De Oliveira Albuquerque et al., 2014). Governance and cybersecurity management will need to move away from compliance to frameworks, standards, and best practices because it does not guarantee governance or cybersecurity, since no known technology or framework, standards, or best practices exist for developing systems and applications without vulnerabilities and risks (De Oliveira Albuquerque et al., 2014). The TJX breach is a case in point of not relying heavily on frameworks, standards, and best practices. The same is true for governance and driving change within organizations, as no known framework, standard, or set of best practices exists that can be applied equally to all organizations.

There is no known framework, standard, or set of best practices that can be applied equally to all organizations. The business within a business issue within organizations is a problem for both governance and cybersecurity management, especially when cybersecurity is integrated within the IT organization. The resulting business orientation and management complexity become a focus due to an overlapping set of structures, frameworks, and processes, characterized by a lack of shared understanding, which is potentially why governance and cybersecurity are generally discussed separately in the literature (Buchwald et al., 2014; De Oliveira Albuquerque et al., 2014). The integration of discussion points is sensible when considering that both governance and cybersecurity frameworks, standards, and best practices tend to focus on information technology management discussions that are similar (Buchwald et

al., 2014; De Oliveira Albuquerque et al., 2014). Both governance and cybersecurity management support business objectives, needs, and processes by minimizing risk and developing trust, while also adopting an iterative approach to continuous improvement (Buchwald et al., 2014; De Oliveira Albuquerque et al., 2014). This can be seen through frameworks such as ITIL, COBIT, and ISO/IEC, as well as SABSA, which are used in governance and cybersecurity management to reduce costs and increase productivity (Buchwald et al., 2014; De Oliveira Albuquerque et al., 2014). However, both governance and cybersecurity management must move away from compliance to frameworks, standards, and best practices by adapting the organization to these frameworks, standards, and best practices, rather than trying to adapt them to the organization.

Moving away from compliance to frameworks, standards, and best practices through the adaptation of these paradigms to the organization's needs should be a primary goal. As noted by Berg et al. (2008), Chandrasekhar (2008), and Xu et al. (2008), being compliant with the PCI-DSS did not help TJX prevent a breach and loss of credit card information. Additionally, Berg et al. (2008), Chandrasekhar (2008), and Xu et al. (2008) suggested that TJX governance was also ineffective. Cherdantseva et al. (2011) have made it clear that the softening of organizational boundaries due to de-perimeterization must be addressed, and ISO/IEC 27000 is not capable of addressing this issue because of its single-organization, closed-system focus. Ahmad et al. (2013) and Ali and Soomro (2014) suggest that ITIL is challenging to deliver due to the overall lack of guidance on what and how. This is echoed by Ahmad et al. (2013), Buchwald et al. (2014), and Weill and Ross (2008) regarding the lack of a shared understanding of governance and its effective delivery. This leads to the general limitation that the current literature lacks an understanding of the need for congruence between governance and cybersecurity management. There is a need for integration of concepts within a modularized, holistic, business-oriented, and risk-driven approach to adapting frameworks to organizations. This approach must cater to organizations across various industries, delivering the value that organizations expect from governance and cybersecurity management.

Assessment of Research Potential

When examining relevant literature across a broad range of topics in governance and cybersecurity management, a consistent conversation emerges concerning both as issues. What is missing in the conversation is the integration of governance and cybersecurity management concepts. Many of the frameworks, standards, and best practices tend to focus on specific areas (PCI-DSS), have little industry specific focus (ITIL), and if not entirely specific to information security (ISO/IEC 27000 series, SABSA) or leave it out entirely (COBIT) (Ali & Soomro, 2014; Burkett, 2012; Cherdantseva et al., 2011; Weill & Ross, 2008). Additionally, many of the issues that cross over from a governance perspective also overlap with the context of cybersecurity management.

Cyberecurity remains a technology issue, in addition to being a non-technical business issue (Burkett, 2012; Cherdantseva et al., 2011). They're not mutually exclusive, and research could focus on global and regional phenomena in the lack of integration and the concept of building cybersecurity into all aspects of technology and business alignment, not just a focus on IT alignment with the business through governance (Weill & Ross, 2008; Weill & Ross, 2009). Future research should focus on the holistic approach to integrating frameworks, standards, and best practices to cover all aspects of business and technology alignment across an organization, regardless of industry. This approach needs to encompass modularity within business-oriented and risk-driven paradigms to ensure the adaptability of frameworks in a holistic manner that suits organizations.

A holistic discussion in the integration of frameworks, standards, and best practices would need to include governance and cybersecurity management within the same conversation. The discussion and research should include the technical and non-technical issues that need to be addressed across governance and cybersecurity management. The

discussion and research need to address the value management issues for measuring the actual costs of impacts resulting from ineffective adaptation versus adapting with the organization in mind. Likewise, further discussion is needed on the impacts of frameworks on governance and cybersecurity management practices within modern businesses to address concerns like those presented by the TJX breach. In this sense, research potential can be expressed as rote compliance relative to systematic adaptation in terms of organizational structure, regulatory concerns, and industry.

Conclusion

Governance and cybersecurity management are key organizational constraints within the modern business environment, particularly when considering the impacts of frameworks. Protecting information resources while delivering on governance and cybersecurity management is an organizational priority. Even though organizations are struggling under the weight of effective cybersecurity management, TJX, for example, they are also having challenges maintaining change management through governance. Even though frameworks, standards, and best practices like ITIL, COBIT, ISO/IEC, and even SABSA can reduce costs while aiding governance and cybersecurity management. COBIT is governance-focused, ITIL is IT service management-focused, and ISO/IEC 27000 series and SABSA are information security-focused (Ahmad et al., 2013; Ali & Soomro, 2014; Burkett, 2012; Cherdantseva et al., 2011). Due to the inherent nature of frameworks, standards, and best practices, organizations should focus less on compliance with them.

Organizations will need to move away from rote compliance practices and adapt frameworks, standards, and best practices to their organizational models and industry to achieve beneficial impacts rather than experiencing harmful ones (TJX). This adaptation relates to the understanding that frameworks, standards, and best practices organizations (such as ISACA, ISO/IEC, and PCI-SSC) have no financial culpability or liability for how their frameworks, standards, and best practices are implemented within an organization (Cherdantseva et al., 2011). This is evidenced by the PCI-SSC not being held accountable with TJX being PCI-DSS compliant even though they were breached utilizing their contractually mandated framework and controls (Berg et al., 2008; Chandrasekhar, 2008; Xu, Grant, Nguyen, & Dai, 2008) Organizations need to integrate and adapt frameworks, standards, and best practices holistically concerning an organization's business model, goals, needs, and requirements for them to be effective. Both governance and cybersecurity management require a level of competence to deliver on their shared goals effectively. Failing to do so will result in poorly implemented governance and cybersecurity management across the frameworks implemented, as the organization attempts to adapt them rather than adapting the frameworks to the organization. The impact can be severe, as seen with TJX.

References

Ahmad, N., Amer, N. T., Qutaifan, F., & Alhilali, A. (2013). Technology adoption model and a road map to successful implementation of ITIL. *Journal of Enterprise Information Management, 26*(5), 553–576.

Ali, A., & Soomro, T. R. (2014). Bridging gape between ITSM, IT-governance and information security to meet business needs. *Research Journal of Applied Sciences, Engineering and Technology, 7*(23), 4906-4909.

Berg, G. G., Freeman, M. S., & Schneider, K. N. (2008). Analyzing the TJ Maxx data security fiasco: Lessons for auditors. *The CPA Journal, 78*(8), 34-37.

Buchwald, A., Urbach, N., & Ahlemann, F. (2014). Business value through controlled IT: Toward an integrated model of IT governance success and its impact. *Journal of Information Technology, 29*(2), 128–147.

Burkett, J. S. (2012). Business security architecture: Weaving information security into your organization's enterprise architecture through SABSA®. *Information Security Journal: A Global Perspective*, *21*(1), 47-54.

Chandrasekhar, R. (2008). Security breach at TJX. London, Ontario: Richard Ivey School of Business.

Cherdantseva, Y., Rana, O., & Hilton, J. (2011). Security architecture in a collaborative de-perimeterised environment: Factors of success. *ISSE Securing Electronic Business Processes, Prague*, 22-23.

De Oliveira Albuquerque, R., García Villalba, L. J., Sandoval Orozco, A. L., Buiati, F., & Kim, T.-H. (2014). A layered trust information security architecture. *Sensors* (Basel, Switzerland), *14*(12), 22754–22772.

Elkhannoubi, H., & Belaissaoui, M. (2016). A framework for an effective cybersecurity strategy implementation. *Journal of Information Assurance & Security*, *11*(4), 233-241.

PCI Security Standards Council (2016). *PCI DSS requirements and security assessment procedures* (ver. 3.2). PCI Security Standards Council. Retrieved from https://www.pcisecuritystandards.org/document_library

PCI Security Standards Council (2008). *PCI DSS requirements and security assessment procedures* (ver. 1.2.1). PCI Security Standards Council. Retrieved from https://www.pcisecuritystandards.org/document_library

Weill, P., & Ross, J. (2008). Mechanisms for implementing IT governance. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results* (Chapter 4, pp. 1–36). Boston, MA: Harvard Business Press.

Weill, P., & Ross, J. W. (2009). Allocating decision rights and accountability: Elements of effective IT governance. In *ITSavvy: What Top Executives Must Know to Go from Pain to Gain*, (Chapter 5, pp. 1–26). Boston, MA: Harvard Business Press.

Xu, W., Grant, G., Nguyen, H., & Dai, X. (2008). Security breach: The case of TJX Companies, Inc. *Communications of the Associate of Information Systems, 23*(31), 575-590.

As a cybersecurity leader, author, and researcher, James is passionate about developing and delivering effective programs. He focuses on assessing and understanding current maturity levels and capabilities and then creating short- and long-term strategies, goals, budgets, metrics, and roadmaps to progress toward higher maturity. The emphasis is on aligning the cybersecurity strategy with the business and technology strategy and integrating it with portfolio, program, and project management.

Background

James is a cybersecurity professional who started in information technology in 1995 and moved into cybersecurity in 2005. James has worked with or within many different industry sectors, including healthcare, FinTech, marketing, skilled trade unions, business process outsourcing, high-end retail, publishing, and manufacturing. Additionally, James has worked with DoD/Fed prime and subcontractors. He was even a paperboy.

Education

James received a Master of Science in Information Assurance and Security in April 2016 (from Capella University), a double major Bachelor of Science in Management and IT Management in March of 2006 (from Kaplan University), a vocational diploma as a Networking and Systems Support Specialist in June of 2000 (from Ridley-Lowell Business and Technical Institute) and a Certificate in the Essentials of Government Contract Management in August of 2013 (from Villanova University). And he cannot say he is done yet because of his philosophy and passion for lifelong learning.

As a working cybersecurity professional, every attempt is made to separate professional and personal endeavors in a manner consistent with reducing conflicts of interest and maintaining ethics. Statements contained within this whitepaper are the explicit and implicit goals, objectives, endorsements, and educated opinion of the author and not those of current or former employers.