INFORMATION SECURITY MANAGEMENT - Insights in the digital context

Introduction

This position paper presents an overview of key insights pertaining to the management of information security in the digital business context, as derived from pertinent academic and practitioner literature. These insights, along with insights from subject matter experts, have informed development of IVI's IT-CMF Information Security Management (ISM) Critical Capability.

Relevance of Information Security Management in the Digital Context

Today's business landscape is characterized by the rapid pace of technological change and growing proliferation and reliance on digital technologies. Evolving business models, greater risk taking and experimentation, enhanced organizational connectivity, and increased information velocity and density are also evident [1]–[4]. All of these changes, together with the growing sophistication of cyber criminals, are key factors for organizations now facing an unprecedented number and range of information security attacks [1] [5]–[10]. It is also anticipated that as more devices, systems, and infrastructure become interconnected and interdependent as a result of digital transformation, and as more interfaces between customers, suppliers, and partners are leveraged, the IT 'attack surface' will continue to expand [5], [11]. Referring to the occurrence of security-related intrusions, Sambamurthy and Zmud [12] outlined that "*the interconnected nature of today's business environment results in ripple effects … severely affecting organizations distant from (and seemingly unrelated to) the early targets*".

Given that the purpose of many cyberattacks is the unauthorized access to, and theft of, corporate or personal data/information, the importance of an effective information security management capability for the organization is paramount. In a recent survey, data loss or destruction was the top rated concern for 41% of enterprise security professionals [5]. Across organizations, the volume of stored data is now growing exponentially due to the unprecedented scale of data collection and 'store everything' practices. This, together with the seamless flow and processing of data across various platforms and applications, increases potential for inappropriate or illegal data/information use or disclosure [5], [11], [13]–[16]. In addition, different organizational functions, regions, verticals, and business ecosystem partners may have different levels of information security maturity [5]. These factors pose a particular challenge for organizations who need to comply with legal and regulatory requirements regarding the secure protection of data/information and reliably demonstrate to organizations and individuals with whom they deal, that they are trustworthy data custodians. Failure to do so can result in regulatory, legislative, financial, and reputational implications that can impact business continuity [7], [17]–[19]. Hence, protecting the organization's key data/information assets must be central to its core operations, in order to preserve their integrity, confidentiality, accessibility, accountability, and usability [8].

[1] Threats faced by organizations include, for example, sophisticated malware, cyber sabotage, phishing, man in the middle attacks, denial of service attacks, brute force attacks, zero day attacks, and ransomware attacks.

Managing Information Security in the Digital Context

Digital business requires a relative[2] view on security that is driven by the organization's risk appetite and risk tolerance set by the leadership team, and that is based on the criticality of business consequences [6], [20], [21]. As such, information security must be solidified as a ***key priority on the C-level agenda*** [20], [21]. CEOs are now expected by their boards of directors and investors to personally know about and be involved in the organization's information security programme [22]. Such board-level involvement, as well as provision of adequate security funding and visible and vocal engagement across the organization, communicates the message that information security is a critical issue with business consequences [5], [22]. The security programme should be driven by a ***clear information security strategy*** that is aligned with the business strategy [6], [20], and supported by ***effective security policies, procedures, and standards*** [21], [22].

The organization needs to evolve its focus on governance - from an IT governance and a tactical information security focus to enterprise digital governance and enterprise accountability [12], [23], and needs to consider where governance of information security should reside within the organization. Many CIOs perceive that governance should rest external to the IT function, with roles such as chief information security officer evident across many organizations [24]. In general, it is accepted that information security is a board level responsibility, and its management needs to be a shared responsibility between all business information users and custodians [20]. Greater communication, collaboration, and an enriched security dialog across departments are required to address information security gaps, as well as a ***partnership-type approach with suppliers, partners, and external agencies*** [5], [12]. Across the entire organization and the wider business ecosystem, a wide range of individual responsibilities must be allocated and clear ownership and accountability assigned, as in the digital age, security is regarded as everyone's responsibility [5], [21].

Development of ***an information security-aware culture is critical*** [7]. In the digital context, there is a requirement for organizations to 'think like the enemy' at all times [20]; hence the concept of security must become engrained within the organizational mindset [5]. Heightened levels of awareness are necessary to keep pace with the types of threat actors at play and to develop new ways to act on insights gleaned from known security breaches [20]. With the advent of social engineering as an effective attack mechanism [25] people-centric information security needs to be emphasized so that employees are not the weak link [7], [12], as unaware or misled users can circumvent even high tech security systems [25]. ***Security awareness training is required for all employees*** [21], [24] as well as specific training initiatives to enhance the skills and professionalism of security teams in emerging security tools and holistic security approaches. Gaps in the talent pool in terms of the technical and operational skillset required should also be addressed to overcome the challenges posed by a lack of security talent [5], [7].

[2] Relative security considers where risks should be mitigated and where they should be accepted (i.e. where the business value exceeds the business risk).

From a tactical perspective, currently organizations are adopting varying approaches in their attempts to prevent security breaches and safeguard their data/information assets from damage, disclosure, or theft: some are overly restrictive making even routine business activities difficult, while others are too relaxed with poor oversight and inadequate protocols and procedures, creating unnecessary exposures. In a recent survey, 88% of respondents believed that their cybersecurity approaches did not meet their organizations' needs and 37% did not have a data protection programme or only had ad hoc policies or processes in place [21]. Understanding the rigidity of security controls, on the spectrum from overly relaxed to overly restrictive, can be difficult as organizational/IT management essentially now need to simultaneously operate in two worlds: "*the world of tight cost management, slow-moving, risk minimization and incremental improvement of old IT, versus the new world of entrepreneurial and creative risk-taking, fast-moving, leading-edge digital*" [26]. In instances where digital leaders strive to embrace experimentation, ambiguity, and uncertainty, and quickly and flexibly react to change [27], the organization needs to ***establish the right balance of controls to secure IT resources without impeding effective business operations***. According to Sambamurthy and Zmud [12], "*the real challenge is to balance the necessity to secure an organization's computer systems, communication systems, and information systems against the necessity for the organization to apply IT productively and creatively in executing and evolving the organization's business models in the face of an ever-changing competitive environment*".

Informed by discussions on risks with the organization's most senior executives and an up-to-date understanding of the evolving threat landscape and the likely threat actors, IT leaders need to ***conduct regular threat and vulnerability assessments and map out threat models*** for the business in order to help determine the rigidity of controls required [7], [23]. Threat scenarios should be evaluated to ensure they are inclusive of all relevant perspectives [20], as the organization needs to effectively handle both predictable threats and unexpected attacks [21], [28]. This process can be enhanced by incorporating external threat intelligence capabilities [21], [23], [25] and participating in relevant industry sharing communities to share and glean valuable insights [20]. The level of risks faced must be continually re-evaluated as security threats and technologies evolve [6], with risk responses being aligned to the magnitude of the risk posed to the organization [20].

In the digital context, organizations are unable to tightly control all possible endpoints due to bring-your-own-device (BYOD) policies and organizational systems being accessed by customers and business partners alike [6]. Hence, a sole focus on perimeter protection and endpoint security is no longer sufficient [6], [7], [20]. Further, a security model that is solely based on complying with standards is inadequate due to the rapid pace of IT innovation and the inability of standards to rapidly evolve in line with technological change [23]. Organizations need to ***re-conceptualize their information security management and adopt holistic, proactive approaches*** that continually adapt to counter emerging threats and minimize the potential negative consequences of exposure [5], [7], [11], [21], [29]. Cognizant of the fact that any weaknesses in security measures are more likely to be exploited over time, the organization needs to continually adapt in line with changing business requirements, and design and implement an industry best practice-informed transformation programme and roadmap to

mature security practices [21], and evolve them from compliance focused, to threat centric and strategic risk focused [7], [23].

Effective information security management in the digital context requires an integral approach covering people, process, and technology [25] and involves a broad spectrum of activities that include anticipation, prevention, protection, detection, and reaction [7]. As a prerequisite, the organization should ***establish a solid foundation of security measures to provide basic defense*** [21] including identity and access management, and measures to secure data centres, applications, databases, and endpoints [7]. The organization also needs to ***shift from solely protecting assets to strengthening them and making them more resilient*** [5]. The security architecture should be revised to reflect ideas regarding depth of defense [20]. Hence, in addition to rich and contextually based access controls, application design and development needs to be security aware [6], [7] and applications need to be effectively protected at run-time [6]. Capabilities for self-testing for vulnerabilities, self-diagnostics of run-time breaches, and self-protection against attacks need to be incorporated within digital technologies. Such self-protecting mechanisms include context-based algorithms for identity management, data isolation through mobile containers, rights management tools, and new monitoring capabilities [6].

In order to improve asset resiliency, IT leaders need to ***keep pace with advances in security technologies*** [20]. The organization needs to look to evolving trends such as cognitive computing/AI, data anonymization, behavioral tracking and analytics, and automation and needs a mechanism for rapidly piloting and implementing such new security technologies and processes. Security teams need to develop innovation and experimentation capabilities to test these new technologies, possibly in a sandbox environment [5].

Finally, organizations also need to ***develop, deploy, and test processes that enable them to anticipate and detect compromises*** to information security and swiftly react to them. This requires a move towards proactive probing, analytics driven event detection and forensics, and reflex-like incident responses [20]. Active defense is a proactive risk-based security approach that involves continually searching for potential attackers and their most likely targets, and based on the data gathered, developing hypotheses about how they are likely to unfold. The insights gleaned enables tailored counter measures to be swiftly implemented to neutralize potential attacks, and facilitates a cycle of continuous learning and improvement that can ultimately lead to improved ROI from security programme investments [25].

Conclusions

Information security is central to the continuity of an organization's business operations and its adherence to legal and regulatory requirements. However, in the digital context a re-conceptualization of information security management is required to enable the organization to address information security threats in more agile and proactive ways. Failure to do so can result in the organization being impacted by high-profile security breaches. Guided by the direction and sponsorship of C-level

executives and clear strategy, policies, procedures, and standards, the organization can build an effective information security capability for the digital context. Inspiring a security-aware culture or mind-set, and ongoing cognisance of external threat intelligence and advances in security technologies are prerequisites for information security success. Similarly, adopting holistic, proactive, and continually adaptive approaches to anticipate, detect, and react to security compromises can enable the organization to more effectively counter emerging threats and minimize the potential negative consequences of exposure.

References

[1] A. Bharadwaj, O.A. El Sawy, P.A. Pavlou, and N. Venkatraman, 'Digital business strategy: toward a next generation of insights', *MIS Quarterly*, vol. 37, no. 2, pp471-482, 2013.

[2] J. Bradley, J. Loucks, J. McCaulay, A. Noronha, and M. Wade, 'Digital vortex - how digital disruption is redefining industries', *Global Centre for Digital Business Transformation*, 2015 [Online] Available: <http://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/digital-vortex-report.pdf>.

[3] T. Catlin, H. Scanlan, and P. Willmott, 'Raising your digital quotient', *McKinsey Quarterly,* 2015. [Online] Available: <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/raising-your-digital-quotient>.

[4] R. Fichman, B. Santos, and E. Zheng, 'Digital innovation as a fundamental and powerful concept in the Information Systems curriculum', *MIS Quarterly*, vol. 38, no. 2, pp329-353, 2014.

[5] Accenture, 'The state of cybersecurity and digital trust 2016 - identifying cybersecurity gaps to rethink state of the art', 2016. [Online] Available: <https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf>.

[6] D.W. Cearley, M.J. Walker, and M. Blosch, 'The top 10 strategic technology trends for 2015', *Gartner*, 2015. [Online] Available: <https://www.gartner.com/doc/2964518/top--strategic-technology-trends>.

[7] CapGemini, 'Address c-level cybersecurity issues to enable and secure digital transformation', 2016. [Online] Available: <https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2017/07/1602_cybersecurity_strategic_consulting_brochure_cc_web_en_1.pdf>.

[8] Frost & Sullivan, 'The 2017 $(ISC)^2$ global information security workforce study – benchmarking workforce capacity and response to cyber risk', 2017. [Online] Available: <https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf>.

[9] M. Mueller, and K. Allan, 'How to use cybersecurity to generate business value', *Ernst & Young,* 2014. [Online] Available:

<http://www.ey.com/Publication/vwLUAssets/EY_CIO_-_How_to_use_cybersecurity_to_generate_business_value/$FILE/EY-CIO-How-to-use-cybersecurity.pdf>.

[10] K. Shepherdson, W. Hioe, and L. Boxall, *88 privacy breaches to beware of: practical data protection tips from real-life experiences.* Marshall Cavendish International, 2016.

[11] PWC, 'Global digital IQ® survey: lessons from digital leaders - 10 attributes driving stronger performance', 2015. [Online] Available: <https://www.pwc.es/es/publicaciones/gestion-empresarial/assets/septima-encuesta-mundial-coeficiente-digital.pdf>.

[12] V. Sambamurthy, and R. Zmud, *Guiding the digital transformation of organizations*. Legerity Digital Press, 2012.

[13] C. Arend, N. Sundby, and A. Venkatraman, 'Reinventing data protection fit for digital transformation', *IDC*, 2016. [Online] Available: <https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA6-8166ENW>.

[14] S. Bosworth, M.E. Kaybay, and E. Whyne, (eds.), *Computer security handbook*. 6th ed. Hoboken, NJ, U.S.A: John Wiley and Sons, 2014.

[15] S. Gutwirth, R. Leenes, and P. De Hert, (eds.), *Data protection on the move - current developments in ICT and privacy/data protection.* Dordrecht: Springer, 2016.

[16] A.N. Sing, M.P. Gupta, and A. Ojha, 'Identifying factors of organizational information security management', *Journal of Enterprise Information Management Decision,* vol. 27, no.5, pp644-667, 2014.

[17] ISACA, 'COBIT 5 for information security', 2012. [Online] Available: <http://www.isaca.org/cobit/pages/info-sec.aspx>.

[18] ISACA, 'COBIT 5 for risk', 2013. [Online] Available: <http://www.isaca.org/cobit/pages/risk-product-page.aspx>.

[19] S. Pental, 'Five ways information security can help IT improve stakeholder engagement', *CEB IT Quarterly – Spotlight on business engagement*. Q2, pp30-33, 2015. [Online] Available: <http://ceb.uberflip.com/i/502110-cio152185syn-rp-q2-it-quarterly-web/33?m4=>.

[20] Accenture, 'Accenture technology vision 2013. Every business is a digital business', 2013. [Online] Available: <https://www.accenture.com/us-en/_acnmedia/Accenture/Conversion-Assets/Microsites/Documents8/Accenture-Technology-Vision-2013.pdf>.

[21] Ernst & Young, 'Creating trust in the digital world - EY's global information security survey 2015', 2015. [Online] Available: <http://www.ey.com/publication/vwluassets/ey-global-information-security-survey-2015/$file/ey-global-information-security-survey-2015.pdf>.

[22] M. Raskino, '10 CEO information and technology resolutions for 2015', *Gartner*, 2015. [Online] Available: <https://www.gartner.com/doc/2973217/-ceo-information-technology-resolutions>.

[23] Accenture, 'Accenture technology vision 2014. Every business is a digital business - from digitally disrupted to digital disrupter', 2014. [Online] Available: <http://investor.accenture.com/~/media/Files/A/Accenture-IR/events-and-presentations/Accenture-Technology-Vision-2014.pdf>.

[24] H. LeHong, S. Prentice, K. Steenstrup, T. Nielsen, and E. Perkins, 'How CIOs need to think about digital business technologies', *Gartner*, 2014. [Online] Available: <https://www.gartner.com/doc/2739917/cios-need-think-digital-business>.

[25] CapGemini Consulting, 'No digital transformation without cybersecurity', 2012. [Online] Available: <https://www.capgemini.com/consulting-nl/wp-content/uploads/sites/33/2017/08/geen_digitale_transformatie_zonder_cybersecurity_0.pdf>.

[26] M. Raskino, 'CEO resolutions for 2014. Time to act on digital business'. *Gartner*, 2014.

[27] J. Peppard, 'Digital dynamics in the C-suite: accelerating digitization with the right conversations', *Sungard*, 2014. [Online] Available: <https://www.sungardas.com/globalassets/_multimedia/document-file/digital-dynamics-in-the-c-suite.pdf>.

[28] O. Lee, and D. Baby, 'Managing dynamic risk in global IT projects: agile risk management using the principles of service-oriented architecture', *International Journal of Information Technology and Decision Making*, vol. 12, no.6, pp1121-1150, 2013.

[29] J. Fraser, B. Simkins, and K. Narvaez, *Implementing enterprise risk management: case studies and best practices.* Hoboken, NJ: Wiley, 2014.

Recommended Reading

Council on Cybersecurity, 'Critical controls for effective cyber defense', *Gartner*, 2013. [Online] Available: <http://www.counciloncybersecurity.org/critical-controls/>.

Joint Task Force Transformation Initiative, 'Security and privacy controls for federal information systems and organizations'. Gaithersburg, MD: National Institute of Standards and Technology, 2013. [Online] Available: <http://dx.doi.org/10.6028/NIST.SP.800-53r4>.

International Organization for Standardization (ISO), 'ISO/IEC 27001: 2013. Information technology security techniques – information security management systems requirements', 2013. [Online] Available: <http://www.iso.org/iso/catalogue_detail?csnumber=54534>.

International Organization for Standardization (ISO), 'ISO/IEC 27002: 2013. Information technology – security techniques – code of practices for information security controls', 2013. [Online] Available: <http://www.iso.org/iso/catalogue_detail?csnumber=54533>.

ISACA, 'COBIT 5 for information security', 2012. [Online] Available: <http://www.isaca.org/cobit/pages/info-sec.aspx>.

National Institute of Standards and Technology, 'Framework for improving critical infrastructure cybersecurity', Version 1.0, 2014. [Online] Available: <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

Office of Cybersecurity and Communications National Cyber Security Division, 'Information technology (IT) security essential body of knowledge (EBK): a competency and functional framework for IT security workforce development', Washington, DC: United States Department of Homeland Security, 2008.

M. Stamp, *Information security: principles and practice.* Hoboken, NJ: Wiley, 2011.

The Open Group, 'Open information security management maturity model (O-ISM3)', 2011. [Online] Available: <https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12238>.

M. Whitman, and H. Mattord, *Principles of information security*. Boston, MA: Cengage Learning, 2011.

Contributing Author

Dr Marian Carcary, Senior Lead Researcher, Innovation Value Institute.

About IVI

The Innovation Value Institute (IVI) is a multi-disciplinary research and education establishment co-founded by Maynooth University and Intel Corporation. IVI researches and develops management frameworks to assist business and IT executives to deliver digitally enabled business innovation. IVI is supported by a global consortium of likeminded peers drawn from a community of public and private sector organizations, academia, analysts, professional associations, independent software vendors, and professional services organizations. Together, this consortium promotes an open ecosystem of research, education, advisory support, international networking, and communities-of-practice. IVI is supported through Enterprise Ireland's and IDA's Technology Centre programme.

Contact IVI

For more information on this capability, IT-CMF and other IT management topics, or on becoming a member of IVI's international research consortium, please visit www.ivi.ie or contact us at: ivi@nuim.ie or +353 (0)1 708 6931.