Introduction

While the era of digital transformation offers organizations considerable opportunities, it is also reflective of significant risks, threats, and uncertainties. The pace of digital transformation, the ongoing evolution of technological trends, and the growing sophistication of cyber criminals result in organizations facing both greater scope and severity of cybersecurity attacks on a daily basis [1]-[5]. These attacks are estimated to cost between $375 and $575 billion per annum [2].

It is anticipated that as more devices, systems, and infrastructure become interconnected and interdependent, and as more interfaces between customers, suppliers, and partners are leveraged, the IT 'attack surface' will continue to expand [1, 6]. The range of threats now faced by organizations is unprecedented and includes, for example, sophisticated malware, cyber espionage, cyber sabotage, phishing, man-in-the-middle attacks, denial of service attacks, brute force attacks, zero day attacks, and ransomware attacks. The actors perpetrating such attacks span hacktivists with political agendas, lone wolf hackers, organized criminal syndicates, state sponsored attackers, external contractors or service providers, or corporate insiders/current employees, among others [1]. In many instances, the purpose of such cyberattacks is the unauthorized access to and theft of corporate or personal data. Across organizations, the volume of stored data is now growing exponentially due to the unprecedented scale of data collection and store everything practices, and this, together with the seamless flow and processing of data across various platforms and applications increases potential for inappropriate or illegal data use or disclosure [1], [6]-[10]. This poses a particular challenge for organizations, particularly in the context of protecting personal and sensitive personal data. Individuals are increasingly aware of their rights under data protection legislation [11]-[13] and those who seek legal redress for inappropriate disclosure of their personal data are successful in approximately fifty percent of cases [14, 15].

Organizations certainly vary in their approaches to attempting to prevent security breaches: 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 [16]. Applying appropriate levels of cybersecurity controls is a particular necessity in the current landscape where digital leaders often now have a higher tolerance and appetite for risk-taking and experimentation to identify key opportunities for the future [17, 18]. As part of the cultural change necessitated, they strive to embrace ambiguity and uncertainty, and quickly and flexibly react to change [19]. Hence, implementing overly restrictive or excessively weak cybersecurity controls can result in regulatory, legislative, financial, and reputational implications that can impact business continuity [2], [20]-[22].

Protection of the organization's computing environment/infrastructure from cyberattacks that can impact business continuity and the organization's protection of key information assets must now be central to its core operations. The organization needs to find the right balance in order to secure its IT resources without impeding effective business operations. In the digital era, it needs to rethink its cybersecurity management approaches [1, 2, 16], and recognize that traditional access control and perimeter defenses alone are no longer sufficient [8]. Rather holistic and proactive approaches that continually evolve and adapt to counter emerging threats and minimize the potential negative consequences of exposure are required [1, 6, 23].

Understanding how effective the organization is in its cybersecurity efforts is a prerequisite for ensuring controls remain abreast of the changing IT threat landscape. The key questions posed by many organizations are 'how secure are our IT assets'? 'are we aware of and responding to the latest threat intelligence'? 'what are our current shortcomings'? and 'what areas do we need to focus on to improve security measures'? This paper presents the Innovation Value Institute's (IVI) Cybersecurity Effectiveness Assessment (CEA), which enables the organization to effectively answer these questions and undertake a targeted roadmap for improvement.

The Cybersecurity Effectiveness Assessment (CEA)

The Cybersecurity Effectiveness Assessment (CEA) provides a holistic analysis of the organization's cybersecurity approaches and identifies key organizational behaviours and technology adoption trends to improve the management of cybersecurity threats. The assessment is industry sector agnostic, suitable for corporations, governments, and not-for-profit entities alike. Assessment participants should include roles that have a broad knowledge of the organization's cybersecurity efforts, for example: chief information officers, chief technology officers, chief security officers, chief information security officers, information security directors, security architects, security auditors, data protection/privacy officers, and network security officers, among others.

This assessment was developed by the Innovation Value Institute (IVI) at Maynooth University, a multi-disciplinary research establishment that focuses on management practices to optimize the business management of IT. The CEA's development is based on a design science methodological approach [24] that reflects the insights of both academic researchers and subject matter experts from IVI's global consortium of public and private sector organizations. The CEA is also firmly grounded in the evolving academic and practitioner discourse on organizational cybersecurity and prerequisites for success.

Core Focus Areas of the Cybersecurity Effectiveness Assessment

The assessment captures insights into a number of core areas:

- The drivers of the organization' cybersecurity programme
- The barriers to the organization's cybersecurity programme
- The threats and threat actors that have impacted the organization in the past 12 months
- The key focus areas of the organization's cybersecurity programme in the next 12 months

- The organization's cybersecurity technology adoption trends
- The organization's cybersecurity management behaviour levels and priorities, detailing the organization's current and future ambition level of achievement across 45 behaviours, grouped into eight themes (Table 1).

Cybersecurity Management Behaviour Theme	Description
Cybersecurity Strategy and Governance	Provide coherent strategic direction and oversight structures to enable effective cybersecurity management.
Cybersecurity Awareness Management	Facilitates responsiveness to intelligence on emerging risks, threats, and vulnerabilities, and to advances in cybersecurity technologies and management approaches.
Technical Security Operations	Establishes security measures to protect all IT solutions, and builds security criteria into their design, development, and delivery.
Data Security Administration	Classifies data and information into security groupings, and provides guidance for managing the security of their life cycles.
Identity and Access Management	Provides the necessary protection levels and access controls to protect against cybersecurity incidents.
Cybersecurity Risk Management	Assesses, prioritizes, treats, and monitors the range of cybersecurity-related risks faced by the organization.
Cybersecurity Incident Management	Detects and addresses the incidents and near incidents resulting from cybersecurity attacks and understands their underlying causes and business impacts.
Business Continuity Management	Ensures the resilience of the organization's operations in the event of a cybersecurity incident.

Table 1: *Cybersecurity Management Behaviour Themes*

Cybersecurity Effectiveness Assessment Process

The CEA is based on a simple online quantitative survey that is targeted to members of the organization's leadership team. The survey findings are validated through tailored qualitative interviews and a prioritization workshop, both of which are facilitated by experienced IT-business advisors. The validated results across each of the assessment areas are compared to available benchmark data across multiple industry sectors. The assessment results are compiled into a logical and easy to understand report that provides the organization with a comprehensive understanding of its current situation as well as clear, prioritized, and measurable improvement recommendations.

Insights Delivered from the Cybersecurity Effectiveness Assessment

Shortlist of Prioritized Capabilities and Recommended Improvements

Providing effective cybersecurity requires the organization to develop a wide-range of capabilities, which will vary in importance depending on the business context and the specific organization's security needs. However, time and resource constraints will undoubtedly challenge organizations that attempt to develop multiple capabilities simultaneously. A key requirement is the need for the organization to focus on developing the capabilities of greatest importance. The CEA outlines not only the most important behaviours to sustain or accelerate further levels of cybersecurity, but also identifies a subset of organizational capabilities associated with the prioritized behaviours. Key recommended improvements in relation to the capability shortlist are also provided (Figure 1).

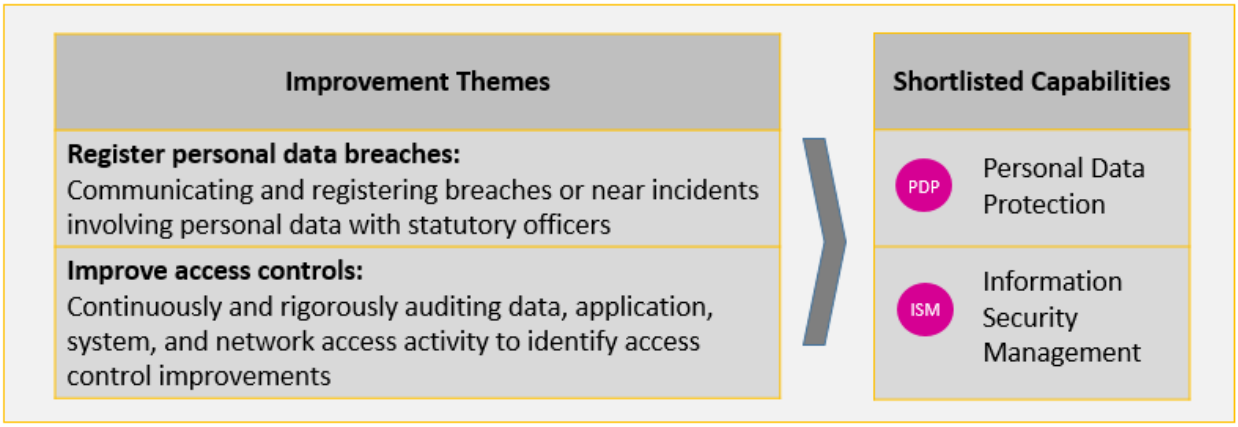

***Figure 1**: Illustrative Example of Prioritized Capabilities and Improvement Themes*

Additional Supporting Tools to Guide Improvements

In addition to identifying a shortlist of capabilities and recommended improvements, IVI provides access to a number of supporting transformation toolkits: IT-Capability Maturity Framework (IT-CMF) [25] and Capability Improvement Programme (CIP) [26].

IT-Capability Maturity Framework (IT-CMF) - Many of the shortlisted capabilities identified in the CEA are drawn from IT-CMF. This represents an integrated management toolkit covering in excess of 30 capabilities associated with the better management of IT (Figure 2). Each capability is broken down into a series of capability building blocks, and has an associated five-level maturity profile and a comprehensive body of knowledge to drive improvement. This includes indicative improvement practices, outcomes and metrics, capability performance indicators, and supporting management artefacts. Currently, organizations on an international basis are using IT-CMF to support the improved business management of IT. This use in turn helps inform the on-going development of IT-CMF, which leverages an open innovation and collaborative research approach between academic researchers and industry-based practitioners – ensuring the principles underpinning the framework are informed by leading insights and best-known practices.

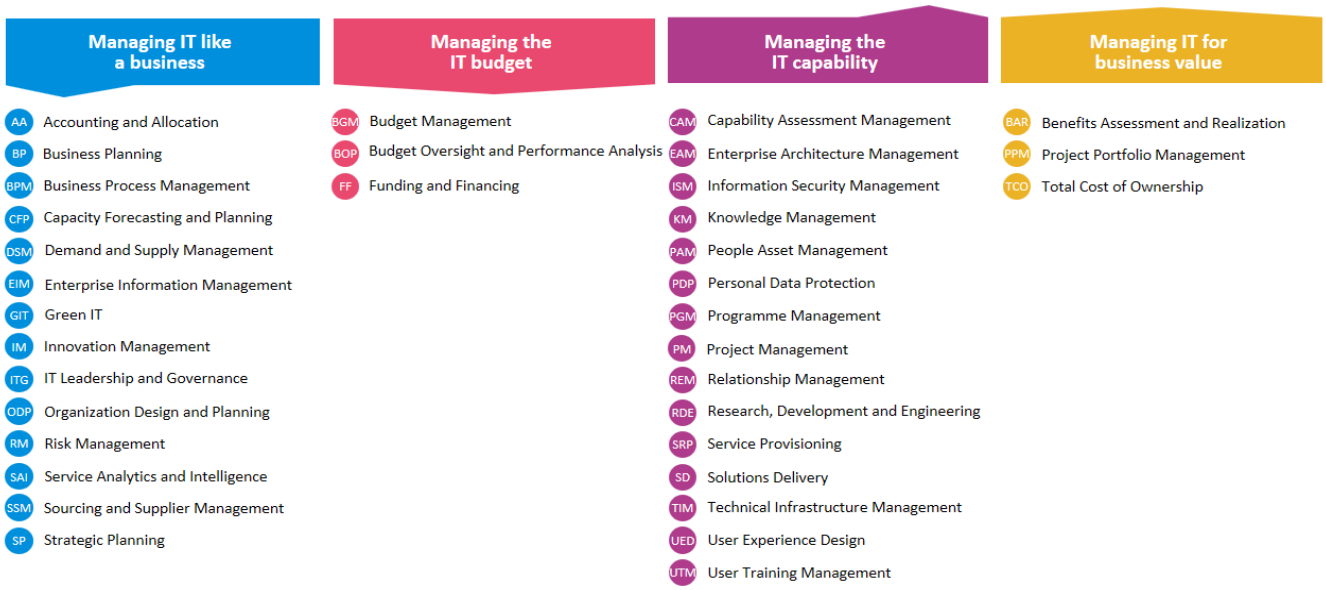

***Figure 2**: IT-Capability Maturity Framework (IT-CMF)*

Capability Improvement Programme (CIP) - The Capability Improvement Programme is a flexible organizational change methodology and toolset designed to facilitate the implementation of IT-CMF. CIP uses best practice change management principles coupled with a structured improvement method that ultimately leads to the execution and the embedding of improvement activities into day-to-day operations. CIP is customized to each organization's specific context and objectives.

Concluding Remarks

Organizations require cybersecurity excellence in order to protect against data theft, destruction, and unauthorized access, comply with legal and regulatory requirements, maintain visibility of the evolving threat landscape, and ensure effective management of actual cybersecurity incidents.

However, they are often impeded due to the absence of strategy, standards, policies, and controls, limitations in the security architecture and cybersecurity management technologies and tools, cultural issues, and resource constraints, among other factors. These barriers result in the ongoing proliferation of high-profile security breaches, with many organizations still unable to detect when or where their systems have been breached – for example, banks and credit card companies notify thousands of businesses each year that their systems have been compromised [27].

CEA Key Value Propositions

The robust, clear, and validated findings of the CEA will help the organization:

- Understand its key strengths and weaknesses in securing its IT assets
- Agree on key cybersecurity drivers and barriers
- Understand the cybersecurity technology trends that will have the greatest impact
- Identify capability gaps in delivering effective cybersecurity
- Identify priority areas to improve and invest in, and gain stakeholder consensus and buy-in
- Implement improvement recommendations in these areas to drive cybersecurity excellence
- Support the culture of change in its cybersecurity management approaches

Due to the disparate needs of organizations across different industries, there is no 'one size fits all solution' to support effective cybersecurity. The insights gained from the CEA serve as the basis for the organization to understand what change it must effect to have in place effective cybersecurity controls that evolve with the changing threat landscape. This serves as the foundation for initiating the organization's cybersecurity improvement roadmap, thereby enabling the organization to develop the structures required to analyse and address continually changing security considerations and take the necessary steps to protect their IT resources proportionate to their organizational value [28, 29].

References

[1] 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>.

[2] 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>.

[3] 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>.

[4] 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.

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

[6] 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>.

[7] 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>.

[8] 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>.

[9] 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.

[10] 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.

[11] BakerHostetler, '2015 international compendium of data privacy laws', 2015. [Online] Available: <http://towerwall.com/wp-content/uploads/2016/02/International-Compendium-of-Data-Privacy-Laws.pdf>.

[12] M. Hildebrandt, and K. de Vries, (eds), *Privacy, due process and the computational turn*. Oxford: Routledge, 2013.

[13] I. Long, *Data protection – the new rules*. Jordan Publishing, 2016.

[14] J. Black, 'Developments in data security breach liability', *The Business Lawyer*, vol. 69, no.1, pp199–207, 2013.

[15] P.N. Howard, and O. Gulyas, *Data breaches in Europe: reported breaches of compromised personal records in Europe, 2005–2014*. Budapest: Center for Media, Data and Society, Central European University, 2014. [Online] Available: <https://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/663/databreachesineurope_1.pdf>.

[16] 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>.

[17] 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>.

[18] 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>.

[19] 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>.

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

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

[22] 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=>.

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

[24] A. Hevner, S. March, and J. Park, 'Design science in information systems research'. *MIS Quarterly,* vol. 28, no. 1, pp75-105, 2004.

[25] M. Curley, J. Kenneally, and M. Carcary (eds), *IT Capability Maturity Framework (IT-CMF) – the body of knowledge guide*. 2nd edition. Van Haren, 2016.

[26] M. Curley, J. Kenneally, M. Carcary, and D. Kavanagh, (eds) (2017). *IT-CMF – a management guide*. Van Haren, 2017.

[27] S. Romanosky, D. Hoffman, and A. Acquisti, 'Empirical analysis of data breach litigation', *Journal of Empirical Legal Studies*, vol. 11, no. 1, pp74–104, 2014.

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

[29] 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>.

Further Reading

European Parliament, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC', 2016. [Online] Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1489407324510&uri=CELEX:32016R0679>.

European Parliament, 'Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA', 2016. [Online] Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1489407324510&uri=CELEX:32016L0680>.

International Organization for Standardization (ISO), 'ISO 31000 – Risk management', 2009. [Online] Available: <http://www.iso.org/iso/home/standards/iso31000.htm>.

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>.

ISACA, ‘COBIT 5 for risk’, 2013. [Online] Available: <http://www.isaca.org/cobit/pages/risk-product-page.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 Government Commerce, *Management of risk – guidance for practitioners*. 3rd ed. London: The Stationery Office, 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>.

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 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 the Cybersecurity Effectiveness Assessment, IT-CMF and other business digitization 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.