Office of the Chief Information Officer

Taking a Risk-Based Approach to Funding Cybersecurity Programs

Introduction

New advancements in information management and information technology (IM/IT) have improved organizational communication and created business opportunities. These advancements must deal with increased exposure to cybersecurity threats, increasingly sophisticated cyberattacks, and greater potential loss. The profound changes in IM/IT require organizations to examine issues (for example, privacy, security, and data protection) in a new way and adapt organizational changes accordingly.

This thought paper explores the following topics:

- Definitions of risk in IM/IT advancement.
- Theoretical and practical considerations of adopting a risk-based approach in cybersecurity.
- Funding cybersecurity programs based on risks and managing cybersecurity threats.
- Current legislative measures and governmental strategies that address increased cybersecurity focus in organization planning.

Defining Risk in Cybersecurity

Investing in cybersecurity programs begins with exploring the fundamental definition of risk. A risk is "an acknowledgment of how likely a threat is to leverage a vulnerability, what the potential impacts could be, and what it means to the organization" (Province of British Columbia, n.d.). Risk in the context of cybersecurity means facing cyber threats such as malware, web-based attacks, and web application attacks (Hoffmann, Napiórkowski, Protasowicki, & Stanik, 2020, p. 657). The International Organization for Standardization (2012) defines "cybersecurity" or "cyberspace security" as "the preservation of confidentiality, integrity and availability of information in the cyberspace."

Risk-Based Approach

Applying a risk-based approach to funding cybersecurity means identifying and assessing risk to prioritize cybersecurity strategies to prevent potential harm from vulnerabilities.

Technological advancement leads to increased sophistication of cyberattacks, pressing organizations to embrace a risk-based approach to cybersecurity to achieve at least a basic level of defensible security (Hale, 2020, p.11). As cybersecurity becomes an essential

part of maintaining business continuity, organizations need to discover and fix security vulnerabilities promptly and consistently to prevent severe financial, environmental, infrastructure, and reputational damage.

A risk-based approach to cybersecurity avoids potentially impeding an organization's operations. Current decision-making approaches often face the dilemma between resolving issues and ensuring business continuity; for example, the need to shut down a web server to address a cybersecurity incident means decreased productivity and availability to the users. This example demonstrates the limitation of static decision-making system by showing the interdependent relationship between confidentiality, integrity, and availability (CIA) of data and information (Qin, Zhang, Zhou, & Xiong, 2018). "The technology industry has experienced a shift toward a proactive, risk-based approach and a better definition of maturity models based on understanding industry baselines and best practices" (Woolward, 2017).

On an organizational level, a risk-based approach in cybersecurity requires the organization's capacity to "identify causes, scope, limits and the type of potential threats of cyber crisis, and develop efficient choice of risk reduction measures, assessment of the transfer validity, acceptance or avoidance of the risk" (Hoffmann et al., 2020, p. 657). Individuals working on a risk-based approach in cybersecurity can apply this thinking and leverage what they are aware of to make reasonable decisions based on the risks. The decisions are particularly helpful when determining what level a cybersecurity program should be funded to and how to allocate budgets. Understanding the risks provides accurate budget projections needed for staff and contractor resources, tools, and risk treatment measures.

What is Risk in Cybersecurity?

In a 1990 report by past Auditor General of Canada, Kenneth Dye advised "the principle of prudence and probity requires that Public Service activities should be transparent and subject to accountability. The underlying aim is to avoid fraud, waste, and abuse, both in fact and in appearance" (p. 195). Taking a risk-based approach to funding cybersecurity programs is consistent with the "principle of prudence" since there is a common aim. The conscious avoidance of fraud, waste, and abuse results in a reduction of risk and helps meet the end goal of risk management.

The traditional method of allocating funds for cybersecurity is often based on compliance regulations and past spending patterns. This approach may not be effective because it fails to consider the ever-changing nature of cyber threats and vulnerabilities.

Organizations can overspend in certain area but neglect more crucial aspects. Using historical spending as a reference does not account for technology advancements that may be more efficient and cost-effective ways of achieving an appropriate level of security.

Therefore, we would recommend organizations use a risk-based approach to funding cybersecurity programs. Funding a risk-based approach to cybersecurity programs involves identifying and prioritizing the most critical assets and systems within an organization and allocating resources to protect them based on the level of risk. This approach maximizes the overall effectiveness of the cybersecurity program by addressing the areas that are most likely to be targeted and would cause the greatest harm if compromised.

A risk-based approach can be applied by assessing potential harmful impact and by determining what the risks means to the organization. When assessing potential impact, establish whether quantitative values can be determined. If not, risk can still be assessed in a qualitative manner; however, quantifying risk helps calculate "return on security investment." In other words, risk determination is a proactive and preventive measure to help organizations to minimize potential loss. Like capability-based planning—a systematic technique that identifies operational capability and uses the most cost-effective option (Coulson, Mason, & Nestler, 2018, p. 2)—the use of a risk-based approach could be extensive and tailored for different organizations.

When taking a risk-based approach to funding a security program, consider the following:

1. Is a treatment action an appropriate use of funds?
2. By applying an investment toward treating a risk, will the treatment reduce the chance of the risk occurring, or the potential impact to the organization if it did?
3. Will an investment result in greater savings to the organization than if the risk occurred?
4. If you let the risk occur without treatment, would this be acceptable to your organization?

Reasonably funding a cybersecurity program commensurate to the scope of the risks and necessary treatments can reduce technical security debt. As services become more reliable due to technical security controls being proactively applied, IM/IT spending also becomes more predictable. Threat intelligence platforms, vulnerability management tools, and incident response teams are examples of an effective strategy to mitigate risk. Another key strategy is to regularly assess and update the organization's cybersecurity strategy to align with the changing vulnerabilities, which include searching and

monitoring for threats, conducting regular penetration tests and incident responses, and establishing a formal incident management process. Additionally, regular testing and training of employees on current cyber threats and best practices helps prevent against social engineering attacks.

Challenges

Implementing a risk-based approach to cybersecurity funding poses challenges, but ones that can be overcome. One major challenge is that it requires organizations to have a thorough understanding of the cyber threats they face as well as the potential impacts of those threats. This knowledge can sometimes be difficult to obtain since the cybersecurity environment is constantly changing, and new threats are emerging. Therefore, a risk-based approach is criticized for being too restrictive as it relates to the range of potential cybersecurity threats.

Another challenge is that implementing a risk-based approach can be resource intensive because it requires ongoing risk assessments and regular updates to the organization's cybersecurity strategy.

Organizations could also potentially struggle to measure the effectiveness of their cybersecurity investments, which augments the difficulty to determine the return on investment for these measures.

These challenges should not discourage organizations from investing in cybersecurity programs. A former director of the United Nations (UN) International Computing Centre authored an article published by ISACA in which he recognized, "Expenditures in information security rarely, if ever, generate revenues. They may add business value in many ways, e.g., reducing the potential occurrence of a security incident, faster resolution of security incidents, supporting the organization's reputation and other intangible areas" (Gelbstein, 2015).

Funding a risk-based cybersecurity program brings significant value to an organization. Such programs can seem abstract, and the value is not always immediately clear. Unfortunately, the value is often not fully recognized, appreciated, or understood by an organization until there is a failure and a major breach or incident occurs. This places the onus on cybersecurity professionals and risk managers to help explain the value to their executive and organization in as clear terms as possible. A risk-based cybersecurity program is important to ensure the organization's goals and objectives are successful, and the day-to-day operations of IT systems remain stable and available with integrity and

confidentiality of data. While a cybersecurity program may not create financial profit for an organization, such a program can certainly result in reduced losses and more predictable and stable expenditures.

Stability means that an organization can plan more reliably—a determining factor in the success or failure of a service. Therefore, IM/IT services should embed security at all life-cycle stages and related risks should be identified and treated. Taking a service design approach for new products and services is important, and security should be part of this. Assessing security risk is a way to determine the proportion of investment put toward a cybersecurity program in support of IM/IT products and services. Consider how an investment in security risk treatments might reduce the likelihood of risks occurring. Coupling this consideration with what the potential impacts would otherwise be, can help quantify the value and rational of related investments.

Governmental Initiatives in Funding Cybersecurity Programs

Even though government initiatives do not explicitly recommend a risk-based approach to cybersecurity, many legislative measures have been implemented to support funding cybersecurity programs.

In 2017, the Consolidated Appropriations Act in the United States directed that an analysis of Federal cybersecurity funding was to be included in the President's Budget. In 2018, the United States passed the SECURE Technology Act. This legislation compelled agencies across their government enterprise to assess cybersecurity risk in their information and communications technology supply chains (White House, 2021, p. 170). These legislative acts accomplished two important milestones for the Unites States:

1. They elevated cybersecurity risk considerations in funding/budgeting at a senior executive level, thereby demonstrating executive commitment.
2. They were followed-up by clear direction to parts of the enterprise of the requirement to assess cybersecurity risk.

Canada has taken a similar but slightly different approach. In June 2022, Public Safety Canada announced Bill C-26, "An Act Respecting Cyber Security (ARCS)." This bill amends Canada's Telecommunication Act to add security as a policy objective. Part of this includes prohibiting the use of high-risk suppliers by Canadian companies, which is a risk-based approach to cybersecurity. This proposed legislation also introduces the Critical Cyber Systems Protection Act (CCSPA), which lays the foundation for securing Canada's critical infrastructure. To comply with this legislation, if passed, designated operators will need to

factor in cybersecurity risk when budgeting, planning, and rolling-out technology through a cybersecurity program. Public Safety Canada's news release suggested that the proposed legislation "could also serve as a model for provinces, territories, and municipalities to help secure their critical infrastructure in collaboration with the federal government" (Public Safety Canada, 2022a).

In the proposed legislation, the Critical Cyber Systems Protection Act explains the purpose "is to help to protect critical cyber systems in order to support the continuity and security of vital services and vital systems by ensuring that, among other things, (a) any cyber security risks in respect of critical cyber systems are identified and managed, including risks associated with supply chains and the use of third-party products and services" (Bill C-26, Part 2, Section 5). The Critical Cyber Systems Protection Act also requires that designated operators "(a) identify and manage any organizational cyber security risks, including risks associated with the designated operator's supply chain and its use of third-party products and service" (Bill C-26, Part 2, Section 9(a)).

In addition, the Canadian government has demonstrated its determination of funding cybersecurity programs by announcing the National Cyber Security Action Plan (2019-2024). Close to $1 billion of federal budget was released in 2018 and 2019 to fund cybersecurity after conducting a comprehensive cyber review (Public Safety Canada, 2022b). The government's objectives include:

1. Building a secure and resilient Canadian systems
2. Forming an innovative and adaptative cyber ecosystem
3. Creating effective leadership, governance, and collaboration

These objectives align with organizations' interest to secure operation and develop adaptability. Organizations in both public and private sectors can benefit from such government-led funding support by investing and developing risk-based approach cybersecurity programs.

Conclusion

In conclusion, recognizing the demand for funded risk-based cybersecurity programs is a must to support successful IM/IT and business operations. A risk-based approach to funding cybersecurity may at times be met with barriers in adoption, and this often can stem from a lack of understanding within an organization. It is more than worth the effort for cybersecurity professionals and risk managers to make the case. Through careful education and awareness, the potential benefits of risk-based cybersecurity programs can

be realized by an organization. These benefits strongly outweigh any countervailing concerns and funding a risk-based cybersecurity program should be pursued to ensure the ongoing stability / availability, confidentiality, and integrity of IM/IT systems and data.

Legislative measures and governmental strategies that prioritize cybersecurity articulate the importance of a risk-based approach in an organization's security planning. As governments adopt initiatives to construct safer and stronger systems through cybersecurity, organizations can leverage learnings and resources to actualize better cybersecurity outcomes themselves. They can implement this by actively participating in the process, using effective funding strategies within their own organizations, and by being open to challenge the status-quo and work toward risk-based cybersecurity programs.

Finally, there are some tangible considerations and actions for organizations as they work toward a risk-based cybersecurity program:

1. Ignoring the problem, or trying to 'fly under the radar' and go unnoticed is not being risk-based.
2. Cybersecurity risk always lies with the organization.
3. Organizations must address cybersecurity risk or have someone do it on their behalf.
4. There is a foundational maturity that must be achieved to address cybersecurity risk; we call this "Defensible Security".
    - This can be achieved by first focusing on hygiene, then compliance, and then risk-based.
    - Many organizations mistakenly view they are operating in a 'risk-based' manner when they are not even 'hygiene' or 'compliance'.
    - If an organization is not at least doing 'hygiene' or 'compliance' then they are failing to ensure an adequate level of security maturity.
    - It is important to have sufficient funding and resourcing for managing security risk.
    - All of this should be guided and supported by risk assessments and a risk register.
    - To learn more about Defensible Security visit: https://www2.gov.bc.ca/gov/content?id=8F737B21C2374B7592B8F5A00A769FCF

References

Bill C-26 (First Reading), *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Session, 44th Parliament, Ottawa, 2022. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/first-reading

Coulson, T., Mason, M., & Nestler, V. (2018). Cyber capability planning and the need for an expanded cybersecurity workforce. *Communications of the IIMA:* Vol. 16: Iss. 2, Article 2. DOI: https://doi.org/10.58729/1941-6687.1401. Retrieved March 6, 2023, from https://scholarworks.lib.csusb.edu/ciima/vol16/iss2/2/

Dye, K. M. (1990, October). *Report of the auditor general to the house of commons for the fiscal year ended 31 March 1990*. https://publications.gc.ca/collections/collection_2015/bvg-oag/FA1-1-1990-eng.pdf

Gelbstein, E. (2015, January). Return on security investment—15 things to consider. *ISACA*, *1*. Retrieved March 6, 2023, from https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/return-on-security-investment15-things-to-consider

Hale, G. (2020, February). Utilities benefit from a risk-based approach to cybersecurity. *Gale Onefile Business*. Retrieved March 31, 2023, from https://go-gale-com.ezproxy.library.uvic.ca/ps/i.do?p=ITBC&u=uvictoria&id=GALE|A628190842&v=2.1&it=r

Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing*, 44, 655-662. https://doi.org/10.1016/j.promfg.2020.02.243

International Organization for Standardization. (2012). Information technology—Security techniques—Guidelines for cybersecurity (ISO/IEC 27032:2012). Retrieved from March 31, 2023, https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

Ministry of Citizens' Services. (n.d.) *Information security glossary*. Province of British Columbia. https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/information-security-glossary

Province of British Columbia. (n.d.). *Concepts*. https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-threat-and-risk-assessment/concepts

Province of British Columbia. (2017, January 16). *Information security risk concepts*. https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-threat-and-risk-assessment/concepts

Public Law 115-390 - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act'' or the ``SECURE Technology Act. *Public and Private Laws. 115th Congress. H.R. 7327. Friday, December 21, 2018.* https://www.govinfo.gov/content/pkg/PLAW-115publ390/pdf/PLAW-115publ390.pdf

Public Safety Canada. (2022a, June 14). Government introduces new legislation to protect Canada's cyber security [Press release]. https://www.canada.ca/en/public-safety-canada/news/2022/06/government-introduces-new-legislation-to-protect-canadas-cyber-security0.html

Public Safety Canada. (2022b, July 25). *National cyber security action plan (2019-2024)*. Retrieved March 6, 2023, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx

Qin, Y., Zhang, Q., Zhou, C., & Xiong, N. (2018). A risk-based dynamic decision-making approach for cybersecurity protection in industrial control systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50*(10), 3863–3870. https://doi.org/10.1109/tsmc.2018.2861715

The White House. (2021). Information Technology and cybersecurity funding. https://www.whitehouse.gov/wp-content/uploads/2021/05/ap_12_it_fy22.pdf

Woolward, M. (2017, May). Risk-based approaches to cybersecurity. *Risk Management, 64*(4), 8+. https://link.gale.com/apps/doc/A491910443/ITBC?u=uvictoria&sid=bookmark-ITBC&xid=e3cdb711