Microsoft

Risk Management for Cybersecurity:

Security Baselines

Authors

Amanda Craig

Contributors

Kaja Ciglic
Angela McKay

© 2018 Microsoft Corporation. All rights reserved. This document is provided "as is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes

Foreword

Technology is empowering people and organizations around the world. In 2017, students in India developed a mobile app that can act as a personal assistant for the visually impaired,[1] and organizations in Africa, Latin America, and Southeast Asia used cloud computing to access affordable banking.[2] But technology is also being exploited by those that use cyberweapons to inflict harm. Botnets have cut off internet service for millions of people, and ransomware attacks have disrupted operations at hospitals and universities. Billons have been lost to cybercriminals.

Recognizing both trends, governments are seeking to realize the benefits of the digital age while managing associated cyber risks. In Europe, for instance, the Directive on security of network and information systems (NIS Directive) is intended to boost cybersecurity across E.U. Member States while supporting continuity across a Digital Single Market. In Singapore, the recently passed Cybersecurity Act aims to protect critical information infrastructure in one of the world's most digitally connected societies.

Microsoft has decades of experience with advancing both innovation and security. We're working on next generation advances in cloud computing, Internet of Things (IoT), mixed reality, and artificial intelligence, unlocking new potential for our customers.[3] Meanwhile, our Digital Crimes Unit is using cloud technologies and advanced analytics to fight cybercrime and improve the security of our products and services.[4] These investments make life tougher for cyber criminals while making people and organizations safer.

We also endeavor to partner with governments as they foster more connected and resilient societies. Around the world, we've built transparency centers to demonstrate the integrity and security of our software to governments.[5] As a technology provider, we also share what we've learned from protecting our own environment and from working with public and private sector customers, law enforcement agencies, and researchers. We want to advance cybersecurity risk management by sharing our experience with government policymakers.

To that end, we are pleased to present this paper, which articulates considerations for governments pursuing efforts to manage cyber risk across sectors and organizations critical to their national resilience. We advocate for a common, foundational approach, sometimes referred to as a "security baseline," that can be used across sectors as well as across geographies. In addition, we describe attributes of effective approaches to security baselines.

In recent years, we've seen that cross-border coordination and public-private partnership are critical to disrupting cybercrime. Going forward, we know that broader coordination across sectors and geographies will drive additional security improvements. We hope that governments consider this paper as they develop and evolve cybersecurity policies and security baselines, working toward a common, foundational approach that supports global alignment and coordination. We look forward to your feedback and continued partnership.

Tom Burt
Corporate Vice President, Customer Security & Trust
Microsoft

---

[1] https://news.microsoft.com/en-in/microsoft-hosts-first-ever-accessibility-summit-india-enhance-technology-access-people-disabilities/
[2] https://blogs.microsoft.com/transform/feature/theres-a-bank-branch-in-your-neighborhood-no-matter-how-remote-it-is/#sm.0012n8sl9sfdcwq10p225ckdxcbf0
[3] https://azure.microsoft.com/en-us/blog/new-innovations-at-microsoft-build-2017-helping-developers-achieve-more/; https://blogs.microsoft.com/iot/2017/09/25/microsoft-ignite-2017-leading-innovation-iot/; https://www.microsoft.com/en-us/hololens; https://www.microsoft.com/en-us/research/research-area/artificial-intelligence/.
[4] https://news.microsoft.com/download/presskits/DCU/docs/dcuFS_160115.pdf
[5] https://enterprise.microsoft.com/en-us/trends/government-security-program-available-to-qualified-governments/

Introduction

Around the world, governments and enterprises are assessing and determining how to most effectively manage a vast array of risks facing their operations. Among those risks, cybersecurity is increasingly important. Information and communications technology (ICT) underpins the functioning of many governments and critical infrastructure organizations, and the complexity of cyber risks continues to intensify. Recognizing this growing need for resilient ICT, organizations of all sizes are evaluating how to manage cybersecurity risks.

In addition to advancing efforts to improve the security of their own operations, governments are developing public policies to advance critical infrastructure cybersecurity. There are dozens of ongoing regional and national initiatives that aim to help critical infrastructure providers manage cybersecurity risks by using "security baselines"[6]. Encouraging, enabling, and, when appropriate, requiring those providers to better manage cyber risks is a sensible government priority. However, there are also many challenges associated with cybersecurity risk management policies, including determining the overall purpose of security baselines, the scope of sectors or services that baselines may apply to, and the policy levers appropriate to foster implementation of baselines.

The approaches that governments take in developing, evolving, and implementing security baselines will have far-reaching impacts. Effective approaches will not only increase both domestic and global security but also support innovation, productivity, and economic opportunity. Less effective approaches will create heavy operational and compliance costs for both businesses and governments without realizing the intended and much-needed security benefits.

This paper responds to three key questions that governments may have as they develop, evolve, and implement security baselines:

- **First,** what are security baselines, and how can they improve cybersecurity risk management across critical sectors? These questions are considered in section one, "Managing risk through security baselines".
- **Second,** how should governments develop security baselines that help governments, critical infrastructure providers, and other enterprises manage risks and make continuous improvements in security? This question is considered in section two, "Developing effective security baselines". Both the processes used to develop effective baselines and the attributes of effective baselines are discussed.
- **Third,** why should governments leverage best practices and global standards for security baselines? This question is considered in section three, "Realizing economic, security, and societal benefits".

[6] Security baselines help organizations manage cybersecurity risk by referencing or describing relevant policies, outcomes, activities, practices, and controls, all of which organizations can use to build their cybersecurity risk management programs. Examples of government initiatives that seek to improve critical infrastructure cybersecurity through the use of security baselines include: the European Union's Directive on security of network and information systems (NIS Directive), China's Cybersecurity Law, Japan's Critical Infrastructure Protection Guidelines, Russia's Law on Critical Information Infrastructure Protection, and Singapore's Cybersecurity Act. Similar developments are ongoing in Chile, Colombia, Kenya, South Africa, Ukraine, Vietnam, and other regions.

Contents

Managing risk through security baselines

What are security baselines?

Security baselines are a foundational set of policies, outcomes, activities, practices, and controls intended to help manage cybersecurity risk. They generally cover a wide range of risk management policy goals, such as protecting against cyber threats or detecting and responding to anomalies or incidents. They can also include more specific desired outcomes (e.g., know your organizational risks), security activities or practices (e.g., conduct a risk assessment; document, review, and disseminate the results; and update the assessment regularly), and security controls[7] (e.g., security policies are defined, approved by management, and communicated to employees and third parties), all of which should contribute to achieving a set of risk management policy goals.

Security baselines are particularly useful in improving cybersecurity because they can cover a range of risks that are applicable across a variety of environments. Most risks faced by governments and enterprises are similar, so most "baseline", or fundamental, risk management activities are also similar. For example, all organizations need to think about regularly reviewing and updating risk assessments, managing how resources are accessed to prevent unauthorized users or behaviors, reviewing event logs to detect events in their infrastructure, and planning for and mitigating the impact of incidents.

While security baselines can address a significant majority of cyber risks applicable across organizations, there may also be risk scenarios that are unique to different sectors or to different business functions within an enterprise. For example, within an enterprise, risks to payment processing systems will likely be somewhat different than those relevant for training systems. In the sectoral context, energy, financial services, and health care companies may also face different risk scenarios or consequences. As such, security baselines that apply across sectors may need to be augmented with a narrow set of guidelines or requirements intended to mitigate the unique risk scenarios relevant to different business functions or sectors.

[7]Security controls are technical, operational, or managerial measures implemented on a system to address security risk.

How can security baselines be used to help manage cyber risks?

Security baselines can be structured and implemented in different ways to help organizations manage broadly applicable cybersecurity risks. Two approaches are important for governments to consider: outcomes-focused and controls-based approaches. While they differ, outcomes-focused and controls-based approaches are complementary, and both can both provide risk management value for organizations.

Outcomes-focused approaches help organizations drive strategic risk management, establishing the necessary processes, capabilities, and investments to address evolving threats and to learn and improve continuously. Compared to a focus on security controls, a focus on security "outcomes" tends to be more easily translatable across different parts of and personnel within an organization, including IT practitioners implementing security for different products and services, incident responders, managers of IT or business functions, and executives. In addition, an outcomes-focussed approach ensures that, in implementation, baselines are suffciently fexible to adapt to changes in technology and the threat landscape.

Controls-based approaches describe security implementation activities that may help organizations address risks. Controls are typically topic specific and technical, providing prescriptive guidance that's narrowly tailored for infrastructure and/or security roles (e.g., network operators or system administrators). Controls describe activities or requirements that respond to basic cybersecurity risks, and they may be particularly useful for organizations that have limited cybersecurity capabilities and would therefore benefit from a clear checklist of activities to do. Common examples of controls-based baselines include International Organization for Standardization (ISO) 27002 and The Center for Internet Security's "Top 20" controls[8].

[8]Center for Internet Security Top 20 controls: https://www.cisecurity.org/critical-controls.cfm

	Outcomes-focussed	Controls-based
Organizational audience	IT and security practitioners, managers, and executives	IT and security practitioners
Overall approach	Strategic approach to risk management establishes "floor" and processes for continuous improvement	Compliance-focussed approach establishes "ceiling" on what should be done for security
Approach to implementation	Describes "what" an organization should do to improve security	Describes "how" an organization should implement security practices
Adaptability	Focus on outcomes rather than on implementation techniques enables adaptability	Focus on technical implementation of prescriptive guidance limits adaptability

Utilizing only or even primarily controls-based approaches has proven insuffcient for managing the cybersecurity risks that organizations face today. In isolation, controls are static and can result in a compliance-based mindset that sets an artifcial and unhelpful "ceiling" on what should be done for security. For example, controls might require an organization to persist in using outdated security practices, even though more effective alternatives have become available. Controls-based approaches have also proven to be a barrier to getting executives to understand and support necessary security investments. On the other hand, outcomes-focused approaches enable organizations to engage a broader internal audience, including executives. They also allow for greater flexibility in adjusting and improving how organizations manage, upgrade, and develop new security techniques by establishing a "floor," or minimum set of expectations for security, that organizations can exceed as new techniques are developed.

Governments can leverage the best of both outcomes-focused and controls-based approaches in developing or evolving security baselines. To do so, an outcomes-focused approach should be the foundation and organizing structure of security baselines, and controls-based approaches should be referenced as guidance where relevant. As desired security outcomes remain relevant as technology and the threat landscape evolve, this structure enables security baselines to be sufficiently adaptable. It also ensures that prescriptive guidance, which may have varying relevance across sectoral or functional contexts as well as dynamic operational environments, is integrated and available for those that would benefit from it. Ultimately, outcomes-focused approaches that reference controls as potential implementation techniques can provide practitioners with guideposts while fostering critical focus on risk management processes, continuous improvement, and strategic security investments.

What sectors or services should security baselines apply to and why?

In the context of public policy, security baselines may apply to a specific sector or across multiple sectors. In our experience, security baselines can easily apply across multiple industry sectors, and there are two significant reasons why governments should adopt such an approach.

First, most cybersecurity risks are similar, and cross-sector baselines will catalyze action immediately and enable sectors to coordinate in managing common issues. Organizations can then focus more attention on the unique risk scenarios that they may need to address with specific mitigations above the baseline.

Second, cross-sector baselines help to address supply chain issues. Many critical infrastructure organizations and governments leverage technologies and resources from multiple organizations in other sectors. These supplier relationships impact both enterprises' and governments' ability to manage security efficiently and to comply with regulatory requirements that extend to third parties. Cross-sectoral baselines enable organizations to pass regulatory or procurement-based requirements to downstream suppliers, helping to create continuity and consistency. Alternatively, fragmentation across sectoral requirements would force organizations to choose to comply with some requirements over other conflicting ones. In addition, a fragmented approach would result in inefficiency as companies and governments seek to demonstrate and assess compliance. To the extent that compliance artifacts can be re-used for multiple customers or regularly assessed in a consistent way by governments, vital resources can be saved and redirected from compliance to security.

As governments develop security baselines that can be used consistently across multiple sectors, they may also consider to which sectors those baselines should apply. Each government must determine for itself which sectors are the most critical to its national resiliency, though many governments prioritize energy, financial services, healthcare, telecommunications and transportation. Moreover, across sectors, governments may take various approaches to implementation, encouraging or enforcing the use of security baselines in different ways—depending on the criticality of the sector and the level of assurance that the government determines is necessary.

How do governments foster use of security baselines?

Depending on an enterprise's maturity and/or a government's needs and resources, security baselines may be implemented through various approaches, including proactively by enterprises themselves or as a result of government initiatives. Mature enterprises may develop baselines or security policies for internal use, just as mature governments may develop baselines to drive security improvements across ministries, departments, and agencies. In addition, governments may foster use of security baselines among critical infrastructure or other enterprises. Where governments have an elevated need for assurance as well as sufficient resources, they may utilize a regulatory approach. In other contexts, governments may find voluntary guidance, coupled with relevant incentives (e.g., procurement requirements), more appropriate, especially in consideration of the costs they incur in developing and ensuring compliance with a regulatory regime. Irrespective of approach, the use of cross-sector security baselines will drive positive behavior beyond those organizations directly impacted by regulatory or voluntary approaches, compelling or incentivizing downstream suppliers of governments or critical infrastructure organizations to implement relevant baseline activities as well.

Developing effective security baselines

A holistic cybersecurity risk management approach is critical to ensuring organizational engagement on tactical, operational, and strategic issues and to enabling continuous improvement. To achieve a holistic approach, organizations must assess and manage cybersecurity risk in the context of overall enterprise risk management. Governments that are developing or evolving security baselines can promote and foster such a holistic cybersecurity risk management approach by focusing on:

I. Utilizing an open, collaborative, and iterative development process;
II. Bridging risk management understanding both within and between organizations;
III. Advancing security through a risk-based and outcomes-focused approach; and
IV. Leveraging existing best practices to the greatest extent practicable.[9]

Below, this paper considers each of the above elements of an effective approach, describing why each is important to risk management as well as valuable to governments and industry.

I. Utilizing an open, collaborative, and iterative development process

In developing or evolving security baselines, a first step for any government is to leverage and integrate the expertise and experience of stakeholders with different backgrounds. Technology is integrated into many systems and services, and stakeholders with different areas of expertise (e.g., technical, business, legal, and policy) and in diverse roles (e.g., civil society, government, and industry) will add unique perspectives that contribute to greater understanding and improved implementation.

The owners and operators of critical infrastructure and of technology products and services are important industry stakeholders in this discussion. In many cases, such stakeholders have developed their own security baselines for internal risk management and adhered to baselines based on external regulatory or procurement requirements. Considering their range of experiences and knowledge about infrastructure and technology systems, they can provide valuable input on how baselines can be implemented, the challenges that must be addressed, and opportunities to drive meaningful improvements.

To leverage and integrate diverse expertise, governments should focus on being open and collaborative, creating an opportunity for the sharing of experiences, perspectives, and ideas. In addition, governments benefit from using an iterative process of policy development, with multiple chances for stakeholders to provide input on drafts, recognizing that the most effective security baselines will be developed and refined over time and with ample opportunity for understanding and incorporating feedback.

[9]See also, https://crx2.org/wp-content/uploads/2018/02/CR2_White_Paper.pdf. Cybersecurity Policy for Resilient Economies: A Global, Cross-Sector Approach describes principles that align with I-IV.

An open, collaborative, and iterative approach can be achieved in various ways. For one, governments can request comments or have a public consultation on shared questions, proposals, or documents. With adequate time (e.g., 60 days) and multiple opportunities to comment on various drafts, organizations can give questions and documents full consideration, provide meaningful feedback, and ensure that their feedback is understood in context. For example, the European Commission and the European Network and Information Security Agency (ENISA) have launched numerous public consultations and surveys, including on how best to partner with the private sector and on the implementation of the NIS Directive.[10]

In addition, governments can host workshops, inviting stakeholders to discuss ideas and provide immediate feedback. In convening government, industry, and civil society stakeholders to develop the *Framework for Improvement Critical Infrastructure Cybersecurity* (Cybersecurity Framework), for instance, the U.S. National Institute of Standards and Technology (NIST) hosted numerous open and collaborative workshops at which it drove conversations around aspects of cybersecurity risk management and effective guidance for critical infrastructure security. In addition, the Singaporean government has hosted workshops to learn about industry perspectives on cybersecurity initiatives.

Alternatively, governments can take a structured but more centralized approach, establishing internal working groups to study globally available best practices and even creating partnerships with peer organizations in other markets before making national proposals. For example, the Cybersecurity Division of Japan's Ministry of Economy, Trade, and Industry (METI) and NIST have jointly supported a research group on the international standardization of cybersecurity. That group is also studying legislation and standardization of cybersecurity technology and submitting to the Japanese government a cybersecurity proposal for local and global industry.

II. Bridging risk management understanding both within and between organizations

A second key step for governments to consider as they develop security baselines is the importance of integrating cybersecurity risk management into broader enterprise risk management communications, processes, and learnings. Risk management guidance consistently highlights the importance of communication across organizations, both horizontally and vertically[11]. However, cybersecurity risk management is a relatively new and technical topic for many company managers, directors, and boards, so they may struggle with both horizontal and vertical engagement on the issue.

[10] https://www.enisa.europa.eu/news/enisa-news/european-commission-opens-public-consultation-on-2018contractual-ppp2019: https://ec.europa.eu/eusurvey/runner/NIS_Dir_IncidentReporting_D

[11] For instance, International Standardization Organization (ISO) 31000:2009 describes how organizations should establish internal communication and reporting mechanisms that support accountability and ownership of risk, enable understanding of risk assessments, and secure support for risk treatments or mitigations.

Security baselines can support communication and bridge understanding across both horizontal and vertical stakeholders, enabling more strategic decision making and informed investments. To support communication and bridge understanding, individuals and organizations must have a "common language": a shared way of interpreting, referencing, and using terms and concepts. In an evolving field like cybersecurity, there is a heightened need to establish such commonality. To do so effectively, a single document or reference point—for example, a set of security baselines—must be understandable to and usable by stakeholders with different expertise and roles, such as security practitioners and business executives within one organization (or even by risk management professionals across multiple organizations).

A common language and single reference point can stitch together the perspectives and interests of stakeholders with varying expertise and roles, which may require different types of information or levels of detail. For example, security practitioners may benefit from more specific instruction as they implement risk management steps to demonstrate compliance with specific controls. Alternatively, executives may benefit from more abstracted information that captures an organization's readiness, resiliency, or maturity in the context of desired security outcomes. A single document that demonstrates the links between both specific and abstracted guidance will be meaningful to both practitioners and executives, acting as a translator for both audiences. Similarly, between or across multiple organizations, a single document can facilitate communication around security learnings or act as a mechanism for suppliers to share information with buyers about their risk management practices.

Bridging cybersecurity risk management understanding across audiences by using common language enables stakeholders to communicate in a meaningful way about the risk landscape, resulting in more informed decisions about how to prioritize and manage risks and creating continuity in security strategy, planning, and investments. If executives can understand what practitioners are aiming to achieve and regularly revisit progress on a relatively consistent set of desired security outcomes, then they may better understand the strategic value of resourcing practitioners to meet goals or to address gaps.

One approach that has been proven to create a common language and to act as an effective bridge both within and between organizations is the Cybersecurity Framework, developed by NIST in partnership with industry and civil society stakeholders[12]. It does so by utilizing five overarching Functions (i.e., identify, protect, detect, respond, and recover), as well as multiple Categories, Subcategories, and Informative References that disaggregate the high-level, strategic Functions into concise statements of desired security outcomes and, where applicable, potentially relevant controls and practices. In this way, executives can quickly digest the purpose of the Functions, and managers or practitioners can utilize the guidance in the Categories, Subcategories, or Informative References that sit within each of those Functions. Ultimately, this mapping enables all interested groups to have a common language and grounded and meaningful dialogue about how to improve organizational performance across or within particular Functions.

[12] https://www.nist.gov/cyberframework

III. Advancing security through a risk-based and outcomes-focused approach

For security baselines to be effective, they must enable enterprises to not only focus on desired security outcomes but also prioritize among the risks and capabilities that are most critical in their environments. Risk-based and outcomes-focused security baselines enable enterprises to have sufficient flexibility as they implement guidance or requirements, allowing their unique infrastructure, operating environment, and business priorities to inform decision-making. In turn, such flexibility means that enterprises can innovate, integrating both security and productivity advancements into products and services that benefit and better protect governments, enterprise customers, and consumers. In addition, in a regulatory or procurement context, risk-based and outcomes-focused security baselines focus government assessments of products or services on meaningful criteria, helping to ensure that governments understand the risks and mitigations that impact their environments.

Risk-based approach: Focus security investments on priority technologies and business functions

In adopting a risk-based approach to security, organizations identify, assess, and manage risk in a prioritized way, recognizing that all activities involve some degree of risk and that no organization has unlimited resources to apply to security. In identifying and assessing risks, organizations focus on vulnerabilities, threats, and consequences: vulnerabilities resulting from people, processes, and technology; internal and external threats; and the consequences of a vulnerability being exploited. In managing risks, organizations determine how to treat the risks that they've identified and assessed, including by accepting, mitigating, transferring (e.g., via insurance), or avoiding risks. In using a risk-based approach, organizations use their processes of identifying and assessing risks to inform decisions about how to manage risks and make security investments, allocating greater organizational and financial resources toward mitigating or transferring more significant risks.

Risk-based security baselines enable organizations to make security investment decisions that best correlate with their risk profiles and business priorities. Different sectors and organizations of various sizes may benefit from investing their security resources differently (e.g., small and large financial institutions may be defending against threat actors with varying resources and goals, necessitating different defensive measures or detection capabilities). Likewise, organizations with different functions or customers may face diverse threats. As such, risk-based security baselines ensure that organizations have the flexibility to make risk management decisions and scale up or down security investments in ways that are consistent with their risk priorities. Risk-based security baselines also enable organizations to balance investments in security with those that support efficient operations and continuous improvement.

In addition to developing risk-based baselines, governments should focus on the most important risks, ensuring that security baselines are as streamlined as possible. While there is value in being comprehensive, doing so can also obfuscate important details, potentially leading to overlooked risks. An all-encompassing approach is also impossible to manage, as it is likely to result in confusion both when organizations attempt to demonstrate compliance and when governments try to assess it. Risk prioritization, by way of contrast, not only helps to ensure that the greatest threats are mitigated, but also focuses attention and increases efficiency in demonstrating security practices and assessing compliance.

Outcomes-focused approach: Enable flexibility to keep pace with dynamic technology and threats

In addition to being risk-based and prioritized, security baselines should be outcomes-focused. As discussed above, both outcomes-focused and controls-based guidance or requirements can have value in cybersecurity risk management. However, governments should structure cross-sector security baselines around security outcomes, articulating what organizations should aim to achieve (e.g., "control logical access to critical resources") rather than how organizations should implement security (e.g., "utilize two-factor authentication"), to ensure that the baselines remain broadly and consistently applicable. Just as desired security outcomes remain more relevant than controls as technology and the threat landscape evolve, so do desired security outcomes remain more relevant than controls across varying sectoral and functional contexts.

Outcomes-focused security baselines are critical to ensuring that both governments and enterprises can utilize the most up-to-date products, services, and security capabilities. As ICT innovation accelerates and threat actors continue to rapidly evolve offensive techniques and strategies, governments and enterprises must also be able to improve their defenses quickly. Rather than being locked in to using technologies or capabilities that were state of the art when a particular control was introduced, governments and enterprises must be able to deploy more secure or convenient solutions as they become available, without the control having to be revised continuously. Outcomes-focused approaches enable such agility.

The rapid pace of and variability among technology developments further contributes to the need for outcomes-focused cross-sector security baselines. For ICT and security organizations to continue to develop and deliver more secure solutions, they must be able to innovate. In addition, as organizations simultaneously work to develop new services with improved security features or new security capabilities, they often take different approaches, resulting in significant variability in the architecture of ICT products or services. Outcomes-focused security baselines enable organizations to have the flexibility needed to implement requirements or guidance in a way that complements those diverse and evolving architectures.

As discussed above, a focus on outcomes in cross-sector baselines also leaves room for sector-specific implementation or "how to" guidance, which should wholly leverage and build on cross-sector security baselines but may also include more prescriptive (i.e., controls-based) guidance as needed. Compared to cross-sector security baselines, sector-specific implementation guidance can also be more rapidly updated by governments and organizations through standards bodies, sector-specific collaborations, or other mechanisms to reflect organizational and industry learnings, changing threat models, and the development of innovative security techniques or capabilities.

A recently published International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) publication, ISO/IEC 27103, is exemplary of an outcomes-focused, cross-sector approach.[13] It is structured around desired security outcomes, including both high-level desired outcomes (e.g., Protect) as well as more specific desired outcomes (e.g. Data at rest is protected). In addition, ISO/IEC 27013 includes a range of ISO, ISO/IEC, and IEC standards, which are mapped to specific desired outcomes, providing greater implementation detail for practitioners to reference. By including not only ISO but also IEC standards, ISO/ IEC 27103 has increased applicability across sectors, and by including international standards exclusively, it is particularly relevant globally.

[13] https://www.iso.org/standard/72437.html; https://webstore.iec.ch/publication/62742

IV. Leveraging existing best practices to the greatest extent practicable

Leveraging existing best practices is the fourth key aspect of an effective approach to developing security baselines. All stakeholders benefit from leveraging existing best practices rather than starting from scratch, including governments. The process of building out a set of risk management practices from scratch is resource intensive. Instead, utilizing tried and tested methods provides governments with a valuable starting point and more immediate results, helping to raise the level of ecosystem cybersecurity and creating opportunities for shared learning and exchange across governments.

Governments can leverage the substance or procedural aspects of existing best practices without emulating methods of enforcement or the exact language or content of a document. For example, a government developing regulatory requirements may recognize the value of a set of best practices that has been implemented through voluntary guidance in other markets. Likewise, a government developing security baselines may find value in the structure and much of the content of an existing best practice but iterate on top of it, making adjustments in a way that is consistent with that government's security or assurance priorities.

Throughout this paper, numerous existing best practices have been referenced. In the context of utilizing an open, collaborative, and iterative process for developing security baselines, this paper referenced best practices implemented by the European Commission, ENISA, NIST, Singapore, and Japan's METI. In addition, the substance of approaches from ISO/IEC 27103, the Center for Internet Security's "Top 20" controls, ISO 27001, and the Cybersecurity Framework have been referenced.

There are also many examples of governments integrating existing best practices as they develop new cybersecurity and risk management policies. The Cybersecurity Framework, for instance, leverages and references ISO 27001, a global standard on information security, as well as Control Objective for Information and Related Technologies (COBIT) and other international and national best practices. Japan's METI[14] has translated and referenced various NIST guidelines and documents for security policy and system operators[15]; The Australian Securities & Investments Commission leveraged and referenced the Cybersecurity Framework in outlining 'health check prompts' to help organizations assess their cyber resilience[16], and Public Safety Canada has noted the relevance and applicability of the Cybersecurity Framework for advancing cyber resiliency among Canadian organizations.[17]

[14] http://www.meti.go.jp/policy/netsecurity/secdoc/ope_contents.html
[15] http://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf
[16] http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf
[17] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx

Realizing economic, security, and societal benefits

In today's world, where people, data, and production constantly flow across borders, leveraging existing best practices is especially critical. In recent decades, global production and trade have resulted in enormous leaps in economic opportunity and technological development. However, if global regulations, including those related to security baselines, fragment or conflict, cross-border flows of resources will be disrupted, negatively impacting growth and potentially curtailing the progress that has been made.

As such, the extent to which governments can synchronize security baselines and build from existing best practices will have profound effects on a range of stakeholders as well broader impacts on societal opportunity, economic development, and global security. For governments, the process of building out a set of risk management practices from scratch is resource intensive and time consuming; for large organizations that operate across borders, having to comply with fragmented compliance requirements diverts resources from security functions; and for local businesses, having to comply with fragmented requirements limits market access. For all stakeholders, fragmentation increases the cost of investing in or leveraging resources across borders. It reverses the global manufacturing and outsourcing relationships that have helped to not only increase global economic opportunity but also drive down the costs of developing and popularizing advanced technologies like smart phones—which, in turn, support new business models and operations across geographies.

Alternatively, focusing on policy alignment and building on existing best practices would help to reduce compliance costs, advance security, and enable greater consistency. Greater alignment of approaches across governments would create continuity and predictability, positively impacting both global and local enterprises. A global organization would have confidence in its ability to leverage resources and operate across borders without unduly burdensome security and compliance costs; as such, it could continue to partner with suppliers or customers across geographies. Likewise, a local organization would have confidence in stable costs as it acts as a supplier of global organizations or invests in new markets. Furthermore, there would be more opportunities for shared learning and exchange across governments and enterprises, and the entire ecosystem would reap security benefits from being able to rely on a culture of effective cross-border cooperation among government authorities and industry stakeholders.

Importantly, as highlighted above, building from existing best practices and focusing on policy alignment does not require that governments emulate the exact content of or methods of enforcing an existing best practice. Rather, governments that start with existing best practices, augment as needed, and contribute to the development of existing best practices further global security.

Government Impact

Globally aligned security baselines are not resource- or time-intensive to develop, so potential security benefits are realized quickly rather than delayed amidst continued dependence on technology for critical functions. In addition, resources are not diverted from building other government skillsets needed to measure and improve the effectiveness of security baselines and ensure enterprises' compliance. Moreover, the invaluable ability to exchange learnings and coordinate with other organizations is realized.

Globally aligned security baselines directly impact the security of ministries, departments, and agencies by enabling them to utilize products and services from a broad set of compliant technology and security providers.

Globally aligned security baselines directly impact small and mid-sized local companies, which can operate beyond their national market more efficiently and leverage technology from a range of suppliers, ensuring access to best-in-class security.

Industry Impact

Globally aligned security baselines ensure that sufficient resources are applied to security and risk management rather than diverted toward compliance. Throughout the ecosystem, the impact of this is multiplied, as third party suppliers are also able to devote sufficient resources to security and risk management rather than diverting those resources toward compliance.

Globally aligned security baselines ensure that organizations continue to invest in security innovation, as organizations have confidence that policies provide sufficient flexibility to develop new techniques, capabilities, and architectures.

Globally aligned security baselines ensure that organizations continue to invest in and leverage resources across borders, maintaining the global manufacturing and outsourcing relationships that have helped to not only increase global economic opportunity but also drive down the costs of developing and popularizing advanced technologies.

Conclusion

Globally, dozens of countries are developing or evolving cybersecurity guidelines, regulations, and standards that reference the need for security baselines for critical infrastructure. How governments approach this effort will profoundly affect global security, societal opportunity, and economic development. Utilizing an open, collaborative, and iterative process to develop an approach that enables risk prioritization, focuses on desired security outcomes, and supports both horizontal and vertical risk conversations will help organizations resource and implement security improvements that are most relevant to their environments and priorities. In addition, utilizing an approach that leverages the substance of existing best practices and is aligned with other governments' efforts will be more efficient and effective for a range of stakeholders. All in all, the results for governments, and their partners in the private sector and beyond, will be improved cybersecurity, both locally and internationally, as well as continued societal opportunity and economic growth.


Microsoft