Aligning security baselines to protect critical infrastructure

Security baselines and cyber risk management

Recognizing their need for secure and resilient information and communication technologies, governments and enterprises of all sizes, including critical infrastructure providers, are evaluating how to manage cybersecurity risks. In addition to advancing efforts to secure their own operations, governments are creating public policies to improve enterprise cybersecurity. There are dozens of ongoing regional and national initiatives that aim to help enterprises manage operational cybersecurity risks by developing or evolving "security baselines". The approaches that governments take in developing security baselines will have far-reaching impacts. Effective approaches will not only increase security, but also enable continued innovation, productivity, and economic opportunity. Less effective approaches will create heavy operational and compliance costs without realizing the intended security benefits.

Understanding security baselines

Security baselines are a foundational set of policies, activities, and practices intended to help manage cybersecurity risk. Baselines cover a wide range of risk management goals, such as protecting against cyber threats as well as detecting and responding to incidents. They may also include more specific desired outcomes or requirements that map to those risk management goals. Security baselines are particularly appropriate and useful in improving cybersecurity because they cover a range of risks that are common across governments and enterprise environments. Because the majority of cyber risks are fairly similar, the majority of security risk management and mitigation are also similar. Where there are risks that are unique to different business functions within an enterprise or to different sectors, security baselines can be augmented with a narrow set of requirements intended to mitigate these unique scenarios.

Adopting an outcomes-based, cross-sector approach to security baselines

As noted above, security baselines often include policies, activities, and practices and may be complemented by more sector-specific requirements, including security controls. For any organization, both controls-based and outcomes-based approaches are helpful in managing risk. Our experience is that baselines that specify what organizations need to achieve (i.e., security outcomes), and do not specify exactly how organizations should implement security (i.e., security controls) are more effective and more likely to have significant, demonstrable impacts on the security of organizations over time. By developing baselines that focus on security outcomes, governments can advance the risk management processes, continuous improvement, and strategic investments that improve enterprises' risk profiles.

Security baselines can also easily apply across industry sectors. Developing security baselines that apply across sectors is a critical step as cross-sector baselines catalyze action immediately, enabling sectors to manage common issues and focus attention on the unique risks they may need to address with measures beyond the baseline. Additionally, many enterprises are horizontally integrated with enterprises from other sectors; similarly, governments utilize products and services from multiple sectors. These supplier relationships impact both the enterprises' and government organizations' ability to comply with regulatory requirements that extend to third parties. Cross-sector baselines therefore heighten the ability of governments and enterprises to assess and demonstrate compliance efficiently.

According to a global Economist Intelligence Unit study, 80% of critical infrastructure providers agree that over the next three years, the proliferation of connected devices, the Internet of Things and Big Data will make them more vulnerable to a serious cyber-attack.

Aligning security baselines to protect critical infrastructure

Developing effective security baselines

A holistic approach, which places online risk in the context of overall enterprise risk management, ensures broad organizational engagement on strategic and tactical cybersecurity considerations and improvements. Effective security baselines tend to adopt the following best practices in their approach or substance:

Leverage diverse expertise by utilizing an open, collaborative, and iterative public policy development process that engages various stakeholders

Through the sharing of experiences, perspectives, and ideas, governments are better positioned to develop baselines that enable improvements in how enterprises manage cybersecurity risk. Iterative processes with multiple chances and ample time for stakeholders to provide input on new draft policies are important. Government entities such as the European Commission, the European Network and Information Security Agency (ENISA), the U.S. National Institute of Standards and Technology (NIST), and Japan's Ministry of Economy, Trade, and Industry (METI) have adopted such approaches either through open consultations or workshops with stakeholders.

Facilitate informed decision-making by bridging risk management understanding both within and between organizations

Especially in an emerging field like cybersecurity, there is a need to establish a "common language"—a common way of understanding and using terms and concepts. To do so, a single document or reference point, like a set of security baselines, must be meaningful for and usable by differently situated audiences, such as security practitioners and business executives. Using a common language to bridge risk management understanding enables stakeholders to communicate in a meaningful way about risk, resulting in more informed decisions about how to prioritize and manage risks and creating continuity in security strategy, planning, and investments.

Manage risk efficiently through a risk-based and prioritized set of baseline practices

Risk-based approaches, grounded in an organization's particular risk and threat landscape, enable organizations to prioritize and focus on security strategies and practices that are likely to have the greatest positive impact on their users. In turn, risk-based security baselines enable organizations to implement a risk-based approach, making decisions that best correlate with their risk and threat landscapes as well as their unique infrastructures and operating environments. Risk prioritization also enables both enterprises and governments to streamline compliance, heightening efficiency and ensuring that assessors can focus on risks of greatest concern.

Enable innovation by driving toward desired security outcomes rather than prescriptive requirements

Security baselines should be outcomes-focused, 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"), which enables government and industry to benefit from continuous security improvement. An outcomes-based approach to baselines also leaves room for sector-specific implementation or "how to" guidance, which may be more prescriptive if needed and allows enterprises the flexibility to regularly update such guidance to reflect the changing technology and threat environments.

Leap forward by leveraging best practices

Rather than building out a set of risk management practices from scratch, utilizing tried and tested methods provides governments with a valuable starting point, helping to quickly raise the level of ecosystem cybersecurity, gaining compliance efficiencies, and creating opportunities for shared learning and exchange. The Cybersecurity Framework, developed by stakeholders convened by the National Institute of Standards and Technology (NIST), is a leading best practice in cyber risk management. It exemplifies a risk-based, outcomes-focused approach that facilitates decision making by establishing a common language.

Support economic growth by realizing economic and security benefits with efficiency

Security baselines are not simply a solution to a technical security challenge. They are an opportunity to improve overall risk management and to support economic growth. Governments benefit from security baselines that are aligned to international best practices through better security outcomes and greater efficiencies. Domestic enterprises are able to grow and compete across jurisdictions while improving security. Consumers enjoy increased safety and consumer protection, lower costs, and wider consumer choice from a global marketplace and product innovations.