GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Tobar, David

"7 Considerations for Cyber Risk Management"

insights.sei.cmu.edu

Carnegie Mellon University, Software Engineering Institute

09 February 2018

URL: https://insights.sei.cmu.edu/insider-threat/2018/02/7-considerations-for-cyber-risk-management.html

Accessed: 02 July 2019

Synopsis: Each year brings new cybersecurity threats, breaches, and previously unknown vulnerabilities in established systems. Even with unprecedented vulnerabilities such as Spectre and Meltdown, the approach to dealing with the risks they pose is the same as ever: sound risk management with systematic processes to assess and respond to risks. This post offers seven considerations for cyber risk management.

Software Engineering Institute

Blogs

7 Considerations for Cyber Risk Management

FEBRUARY 9, 2018 • INSIDER THREAT BLOG

By David Tobar (/author/david-tobar)

Mission Assurance (https://insights.sei.cmu.edu/insider-threat/mission-assurance/)

Each year brings new cybersecurity threats, breaches, and previously unknown vulnerabilities in established systems. Even with unprecedented vulnerabilities such as Spectre and Meltdown, the approach to dealing with the risks they pose is the same as ever: sound risk management with systematic processes to assess and respond to risks. This post offers seven considerations for cyber risk management.

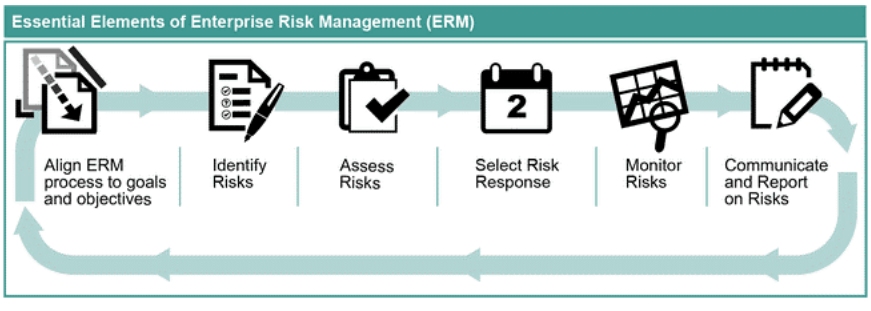
What Is Cyber Risk Management?

The International Organization for Standardization (ISO) defines *risk* as the "effect of uncertainty on objectives (https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1)." *Risk management* is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should assess the likelihood and potential impact of an event and then determine the best approach to deal with the risks: avoid, transfer, accept, or mitigate. To mitigate risks, an organization must ultimately determine what kinds of security controls (prevent, deter, detect, correct, etc.) to apply. Not all risks can be eliminated, and no organization has an unlimited budget or enough personnel to combat all risks. Risk management is about managing the effects of uncertainty on organizational objectives in a way that makes the most effective and efficient use of limited resources.

A good risk management program should establish clear communications and situational awareness about risks. This allows risk decisions to be well informed, well considered, and made in the context of organizational objectives, such as opportunities to support the organization's mission or seek business rewards. Risk management should take a broad view of risks across an organization to inform resource allocation, better manage risks, and enable accountability. Ideally, risk management helps identify risks early and implement appropriate mitigations to prevent incidents or attenuate their impact.

Essential Elements

Most risk management standards, such as those from ISO (https://www.iso.org/iso-31000-risk-management.html), COSO (https://www.coso.org/Pages/erm-integratedframework.aspx), and NIST (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf), and have common key processes. In its best practices for an enterprise risk management program (https://www.gao.gov/assets/690/681342.pdf), the Government Accountability Office (GAO) identified six essential elements:



Source: GAO. | GAO-17-63

The first element, aligning enterprise risk management to goals and objectives, sets the foundation for the program by establishing the three pillars of enterprise cyber risk management (https://insights.sei.cmu.edu/insider-threat/2017/11/the-3-pillars-of-enterprise-cyber-risk-management.html): governance, risk appetite, and policy and procedure. *Governance* should include a body of risk-decision experts and decision makers using a framework of risk management processes that ensure engagement by key stakeholders (leaders, Authorizing Officials, and Risk Committee). *Appetite for risks* should be aligned to organizational goals and objectives. *Policies and procedures* communicate risk management expectations, risk definitions, and guidance throughout the enterprise. Once the risk management program is running, the remaining five elements continuously manage risk.

Seven Considerations for Cyber Risk Management

The following seven topics are well worth considering when planning a risk management program.

1. **Culture.** Leaders should establish a culture of cybersecurity and risk management throughout the organization. By defining a governance structure and communicating intent and expectations, leaders and managers ensure appropriate leadership involvement, accountability, and training. That last one is critical: ongoing training is required to maintain expertise and deal with new risks.
2. **Information sharing.** Security is a team sport. The right stakeholders must be aware of risks, particularly of cross-cutting and shared risks, and be involved in decision making. Communication processes should include thresholds and criteria for communicating about and escalating risks. The potential business impact of cyber risks should be made clear. Information-sharing tools, such as dashboards of relevant metrics, can keep stakeholders aware and involved.
3. **Priorities.** All organizations have limited budget and staff. To prioritize risks and responses, you need information, such as trends over time, potential impact, time horizon for impact, and when a risk will likely materialize (near term, mid term, or long term). This information will enable comparisons of risks.
4. **Resilience.** We can't guarantee success in protecting against all risks. Risk management must also enable continuity of critical missions during and after disruptive or destructive events, including cyber attack. Resilience is an emergent property of an entity to be able to continue to operate and perform its mission under operational stress and disruption. Many organizations use the CERT Resilience Management Model (CERT-RMM) (https://www.cert.org/resilience/products-services/cert-rmm/index.cfm) to manage and improve their operational resilience. The model includes Risk Management as one of its 26 process areas.
5. **Speed.** When an organization is exposed to a risk, speedy response can minimize impact. Identifying risks early helps. Incident response and recovery depend on planning and preparation for incident management. Incident management plans should be exercised periodically.
6. **Threat environment.** Cybersecurity does not always pay enough attention to the threat environment. Organizations should improve their intelligence into adversary capabilities (consider network security sensors and other reporting) while also accounting for risks from third parties (supply chain) and insider threats. Insiders, whether malicious or inadvertent (such as phishing victims), are the cause of most security problems.
7. **Cyber hygiene.** Implementing basic cyber hygiene practices is a good starting point for cyber risk management. Cyber hygiene focuses on basic activities to secure infrastructure, prevent attacks, and reduce risks. The Center for Internet Security (CIS) has a list of 20 cybersecurity controls (https://www.cisecurity.org/controls). The SEI recently released a baseline set of 11 cyber hygiene practices (https://resources.sei.cmu.edu/asset_files/Presentation/2017_017_001_508771.pdf). When implementing hygiene practices, start by improving your knowledge of your own high-value services and assets. These require additional protection, including enhanced access controls and system monitoring. Read more in our blog post on cyber hygiene (https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html).

Prepared, Not Bullet Proof

With cyber risks continuing to grow, making good risk management decisions really matters. Rushing through decision making and always saying "no" are not the right answers. A better answer is to implement a consistent risk management program. Cyber events will still happen to your organization, but it will be better prepared to deal with them.

For more information about risk and resilience in your organization, see http://cert.org/resilience/ (http://cert.org/resilience/) or contact me at info@sei.cmu.edu (mailto:info@sei.cmu.edu).

About the Author

David Tobar

Contact (https://www.sei.cmu.edu/contact-us/index.cfm?f=David&l=Tobar)

View all blog posts » (/author/david-tobar)
View other publications » (http://resources.sei.cmu.edu/library/author.cfm?authorID=446122)

Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
412-268-5800