TruOps
Cyber Risk Management

55 North Water Street | Norwalk, CT 06854
203.866.8886 | truops.com

Three Key Areas for Achieving Cyber Resilience

Mitigating cyber risk remains a major area of concern for private organizations, government agencies, and even Joe Citizen. A 2018 Gallup poll revealed that among the 13 crimes measured, cybercrimes were most feared by Americans. Seventy-one percent of poll participants stated that they "frequently or occasionally" feared that computer hackers would access their personal, credit card, or financial information. Sixty-seven percent worried to the same degree about identity theft.[1]

The federal government has been leading initiatives to stay one step ahead of cybercriminals. At the 2019 USA RSA Conference in March, the director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) indicated that the agency is focused on several key priorities for protecting the country's critical IT infrastructure. By modeling the government's efforts to combat cyber threats, commercial enterprises can also enhance their situational awareness, reduce risk, and achieve cyber resilience.

What is Cyber Resilience?

Cyber resilience is defined as "an entity's ability to continuously deliver the intended outcome despite adverse cyber events."[2] The 2013 Policy Directive (PPD) on Critical Infrastructure Security and Resilience defines resilience as the "ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions."[3] In this day and age, all IT systems, critical infrastructure, business processes, and government and commercial organizations should have cyber resilience capabilities. Resilience encompasses not only the ability to withstand and recover from deliberate cyber attacks, but also from accidents and naturally occurring threats or incidents.

All IT systems should have **CYBER RESILIENCE CAPABILITIES.**

During the 2019 USA RSA Conference, CISA director Christopher Krebs discussed the National Risk Management Center's role in creating a cross-sector risk management approach across the federal government and its private sector partners to identify and prioritize strategic risks, integrate government and industry activities in the development of risk management, and synchronize operational risk management activities. Krebs outlined three key focus areas for the agency: protecting the nation's supply chain, reducing the surface attack area, using threat intelligence, and information sharing.

Cyber Resilience Focus Area 1: Protecting the Supply Chain

A supply chain attack occurs when a third party gains unauthorized access to an organization's systems and data. As more companies share sensitive data with third-party vendors out of business necessity, this vector of attack has become more prevalent. The cybersecurity technology company Symantec revealed in its annual report on Internet security threats that supply chain attacks significantly increased by 78% between 2017 and 2018.[4]

Third-party risk is a critical cyber security issue, and forward-thinking companies have established teams solely for managing this issue. Although stories about breaches affecting the retailer Target, the credit agency Equifax, and other large corporations have grabbed headlines in the past, all organizations regardless of size and sector should have a plan and process for assessing and mitigating their third-party risk. The 2017 Ponemon Institute study, Data Risk in the Third-Party Ecosystem, indicated that 56% of organizations had experienced a breach caused by one of their vendors. The average number of third parties with access to sensitive data at each company surveyed had increased from 378 to 471. Only 35% of companies polled reported having a list of all the third parties with whom they shared information. Just 18% of companies stated they were aware if those vendors had been sharing that information with other suppliers.[5]

For good reason, organizations are paying greater attention to assessing and managing the risk posed by third-party relationships. The following year, in 2018, the Ponemon Institute published Measuring & Monitoring the Cyber Risks to Business Operations. The report found that 64% of IT professionals surveyed saw unauthorized sharing of confidential data by third parties as the second most pressing security worry for 2019. Forty-one percent said they had dealt with security events related to third-party relationships in the past 24 months.[6]

Cyber Resilience Focus Area 2: Reducing the Attack Surface

In cyber security, an attack surface is the number of vulnerabilities that can be exploited to carry out a cyberattack. Whether physical or digital, attack surfaces should be limited in size to prevent unauthorized, harmful access. One of the most effective ways to limit the attack surface is by eliminating unnecessary complexity in security infrastructure and policy. The more steps required to execute tasks, the more likely human error and risk will enter.

Attack surface modeling, attack simulation, and patch simulation are methods for visualizing vulnerabilities utilizing a real-time model of what might happen in the context of network movement when a cybercriminal attacks a vulnerability. Additional strategies for reducing the attack surface encompass monitoring and controlling network endpoints, segmenting networks, and prioritizing analytics. Still other effective tactics organizations can employ to reduce the attack surface include: ensuring that security tools are enabled and other services are secure by default; uninstalling unneeded software; leveraging memory randomization and tools to enhance the system's ability to protect itself; developing secure applications, sandboxing and containing threats; and documenting and analyzing malicious code.

Cyber Resilience Focus Area 3: Using and Sharing Threat Intelligence

Cyber threats occur on a daily basis at warp speed. Oftentimes it isn't a matter of if an organization will face a security breach, but when. No one organization can possibly gauge the level of threat activity by nameless, faceless cybercriminals. Organizations should look to increase their use of threat intelligence and be willing to share what they learn with the cyberthreat intelligence community at large. This can be done by partnering with trusted open source threat intelligence sources and joining the Department of Homeland Security's (DHS) Automated Indicator Sharing (AIS) program.[7] According to the DHS, this free service facilitates the exchange of cyber threat indicators between the federal government and private sector at machine speed. Examples of threat indicators are pieces of data, such as malicious IP addresses or the sender address of a phishing email. CISA is in the process of refining the AIS program to include more context and specificity to deliver more value-added threat intelligence to the private sector.

> *Organizations should look to increase their use of* **THREAT INTELLIGENCE** *and be willing to share what they learn.*

Threat information that has been aggregated from multiple sources and vetted is highly valuable and actionable. To facilitate the availability of high-level intelligence to small- and medium-sized businesses, the Cyber Threat Alliance (CTA) was formed by a consortium of members from the cybersecurity industry, including Fortinet, McAfee, Symantec, and Palo Alto Networks. The Alliance recognizes the critical need for security professionals to have access to the intelligence and technology tools they need to identify and stop cyberattacks in their tracks. The CTA is dedicated to improving the cybersecurity of its global digital ecosystem by significantly reducing time to detection and closing the gap in the detection-to-deployment lifecycle. This is facilitated through the sharing of near real-time, high-quality cyber threat information and operational coordination between companies and organizations in the cybersecurity field.[8]

Best Practices for Building Cyber Resilience

For organizations to achieve the level of cyber awareness needed to build resilience, the following best practices should be part of an overarching risk management strategy:

- **Create a Response Plan for Threat Incidents:** Leveraging a data-driven approach and advanced threat intelligence enables organizations to better identify potential attacks and develop a more proactive response plan for the enterprise. The response plan should clearly outline the actions that should be taken when a threat incident occurs.
- **Monitor Systems Continuously to Identify Attacks:** Networks and information systems should be continually monitored to identify threat incidents before they can cause any significant damage. Any detected anomalies and vulnerabilities should be addressed in accordance with the organizational response plan.
- **Deploy Plans and Systems to Restore Affected Data:** Recovery is a mission-critical component of any cyber resilience plan. It involves developing and deploying the necessary plans and systems to restore any data and services that have been impacted during a cyberattack as quickly as possible.

Cyber Resilience Is a Collective Effort

The cyber threat landscape is becoming more complex and sophisticated with each passing day, putting companies at risk for being breached. Organizations seeking to thrive and survive in this environment must make building cyber resilience an enterprise-wide culture and mindset. Although cyber resilience is an organizational effort supported by people, processes, and technology, it does not—and should not—exist in a vacuum. Cyber resilience is also about the larger digital ecosystem and the exercise of cyber corporate citizenship. Both public and private organizations have a vested interest in supporting the digital ecosystem, which requires being proactive in identifying and remediating attacks, as well as sharing threat intelligence publicly. By working cooperatively, commercial enterprises and government agencies can improve their cyber resilience collectively.

References

1. https://news.gallup.com/poll/244676/cybercrimes-remain-worrisome-americans.aspx
2. https://en.wikipedia.org/wiki/Cyber_resilience
3. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
4. https://www.symantec.com/security-center/threat-report?om_ext_cid=biz_vnty_istr-24_multi_v10195
5. https://www.opus.com/ponemon-2017/
6. https://www.tenable.com/ponemon-report/cyber-risk
7. https://www.dhs.gov/cisa/automated-indicator-sharing-ais
8. https://www.cyberthreatalliance.org/value-collaborative-threat-intelligence-sharing/

TruOps

Cyber Risk Management

55 North Water Street
Norwalk, CT 06854

203.866.8886 | truops.com