Take These 5 Steps To Help Prepare for Growing Cyber Threats

Risk managers already face a plethora of challenges as they seek risk resilience, including balancing rising rates with shrinking corporate risk budgets. Now, they can add increasingly sophisticated cyber attacks and the rising cost of cyber risk to the list of challenges.

Rising cyber threats are increasing both the difficulty and the importance of risk managers' efforts to take control of their risk. Cyber risk is no longer solely a technology issue but also an enterprise risk issue, and it's coming under heightened scrutiny from the C-suite, the boardroom and investors.

As a result, risk managers and their organizations have a duty to understand both cyber perils and their growing threat to business continuity and customer data, and how cyber losses and the increasing costs of cyber insurance in the risk transfer markets affect their risk management programs.

The disruption to businesses' growth, competitiveness, operations and existence continues to play out and will dramatically increase in the coming years. No industry, business or business segment is immune:

Ransomware remains a heightened concern, and for good reason: Attacks are up 716% from 2019 to 2020, with predicted damages from attacks expected to cost

$20 billion

in 2021.[1]

The widespread 2020 attack on SolarWinds,

attributed to foreign nation-state threat actors, targeted supply chains, and affected public and private organizations around the world.[2]

Attackers are increasingly intercepting

money transfers, stealing sensitive commercial strategies and intellectual property (IP), and running extortion schemes.[3]

The FBI reports that cyber attacks are

up 400%

from pre-COVID-19 pandemic levels.[4]

Cyber crime has certainly caught the attention of organizational leaders as threat actors continue to develop sophisticated business models to monetize and profit from exploiting technical and human vulnerabilities. Many organizations have much work to do:

The human factor in cyber attacks continues to be a concern, with employee and user actions accounting for

30%

of all data breaches.[5]

IP theft is estimated to be a

$1 trillion problem,

yet just one-third of companies protect trade secrets.[6]

C-suite executives continue to be prime targets for attacks: They are

12 times more likely

to be pursued and nine times more likely to be victimized.[7]

The need for thorough cyber due diligence is

critical

in any M&A activity.[8]

The Increasing Cost of Cyber Risk

As cyber attacks have risen in frequency and severity, so have insurance losses. The days of inexpensive cyber insurance coverage have ended. Insurers are under extreme pressure to increase rates, tighten underwriting criteria and restrict capacity — or even exit the cyber market entirely — as cyber insurance combined ratios have risen dramatically.

Companies can anticipate rate increases as high as 80% into 2022 as carriers work to atone for growing losses in their cyber-risk books of business.[9]

5 Basic Fundamentals that Risk Managers Should Ensure are Implemented

□ 1. **Create a multidisciplinary committee for cyber risk management:** The impact of cyber risk can be felt across every department in a business — from legal to compliance, human resources, finance, communications, operations, information technology and elsewhere. A cyber risk committee is a relatively low cost organizational change that brings together the relevant expertise to assess how cyber risk will impact multiple functions, and how changes in the business — such as an M&A transaction, working with a new vendor, or implementing new technologies — will alter the security posture. The General Counsel, who has an apolitical position in the organization, as well as familiarity with the regulatory environment and downstream liabilities should chair this multidisciplinary committee and report out to the CEO and Board with their findings.

□ 2. **Conduct a security assessment:** The best way to understand the current state of a company's security, is to conduct an independent security assessment. Smaller organizations with less complex systems may consider SaaS-based solutions, which can be cheaper and allow IT or information security leaders to input information and receive an instant score on their security posture. The results of the assessment should then be shared with the multidisciplinary committee so as to inform where budget is spent to close gaps, prioritize critical data and assets for protection, and what to insure. Investing in red team exercises[10] will help expose weakness and identify priorities for remediation before a real attack can strike.

□ 3. **Create a culture of security:** Weaponize your employees in the fight against cyber crime by investing in the right training and awareness programs, with a focus on engaging programs that change human behavior. No one should be exempt from these exercises — including the board and senior executives. For example, proactively teaching people how to spot suspicious phishing emails as well as implementing better password management practices. These small security strategies can have an immediate positive effect.

□ 4. **Incident response planning:** Incident response planning focuses on improving the company's resilience in the face of attacks.[11] Many companies now have an incident response plan, but it's important to test the plan with all stakeholders involved and keep it regularly updated. Planning for an incident — particularly ransomware — also involves creating regular back-ups of critical data and systems to reduce downtime, and testing defenses, all by simulating attacks.

□ 5. **Have a tailored cyber insurance policy:** Even after taking a number of proactive steps such as those outlined above, the evolving threat landscape means that no company can be completely secure. It's important to ensure that any cyber insurance policy considers the risk exposures of greatest concern to the company, as there is no "one size fits all" from a coverage standpoint. A cyber policy should always be treated as part of a broader cyber security strategy that has, at its heart, a proactive approach to risk mitigation.

This material has been prepared for informational purposes only and should not be relied on for any other purpose. You should consult with your own legal and information security advisors or IT department before implementing any recommendation or guidance provided herein.

[1] Chad Pinson, Jonathan Rajewski, and Stephanie Snyder, "The Ransomware Epidemic," Aon, October 29, 2020, https://www.aon.com/cyber-solutions/thinking/client-alert-the-ransomware-epidemic/.

[2] "Security Advisory — SolarWinds Orion Breach," Aon, December 15, 2020, https://www.aon.com/cyber-solutions/thinking/urgent-security-advisory-solarwinds-orion-breach/.

[3] Aon, 2020 Cyber Security Risk Report – Solving The Cyber Puzzle: The Unexpected Ways Cyber Risk Impacts Your Business, February 2020, https://www.aon.com/report-cyber-risk-data-breach-impact-to-organization-ip-mergers-acquisitions-security-threats/index.html.

[4] Maggie Miller, "FBI sees spike in cyber crime reports during coronavirus pandemic," Hill, April 16, 2020, https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic.

[5] 2020 Verizon DBIR Report

[6] Aon, 2020 Cyber Security Risk Report.

[7] Aon, 2020 Cyber Security Risk Report.

[8] Aon, 2020 Cyber Security Risk Report.

[9] "Midyear 2021 Errors & Omissions | Cyber Insurance Snapshot," Aon, October 1, 2021, https://www.aon.com/cyber-solutions/thinking/midyear-2021-errors-omissions-cyber-insurance-snapshot/.

[10] "How To Choose Your Red Team Vendor," Aon, October 11, 2020, https://www.aon.com/cyber-solutions/thinking/how-choose-your-red-team-vendor/.

[11] "5 Steps to Help Get Cyber Incident Response Right for Your Business," Aon, https://insights-north-america.aon.com/mtcor/5-steps-to-help-get-cyber-incident-response-right-for-your-business.