Cybersecurity considerations for executives and boards of directors: How recent cyberattack trends and developments inform strategies for reducing cyber-risk

Focus on the healthcare sector

23 August 2021
By: Lori Marsh | Emily Maus | Anna Spencer

As more organizations shift to remote work in light of the COVID-19 pandemic, cybersecurity has become top of mind for companies across all industries. A newly remote world has increased organizations' reliance on digital records, controls and technologies, making them rich targets for ransomware attacks.

Healthcare businesses, like those in other high-risk sectors, are coming to appreciate the need for greater investment in data governance, risk management and compliance programs.

In this alert, we review recent trends and costs associated with cyberattacks and analyze how organizations can implement strategies for reducing cyber-risk.

Global costs of data breaches are on the rise

A study published this summer by the Ponemon Institute and sponsored and analyzed by IBM Security, which combined results across 17 industries, including 537 organizations from 17 countries and regions, highlighted that the global average total cost of a data breach is $4.24 million. The report concluded that the industries with the highest average data breach costs are the healthcare, financial services, pharmaceutical, technology and energy industries. For the past 11 consecutive years, healthcare organizations experienced the highest average cost of a data breach. Between 2020 and 2021 alone, these costs increased 29.5 percent.

In light of these statistics, among other potential strategies for reducing risks associated with cyberattacks, organizations should consider strengthening their information security programs, maintaining cyber insurance and implementing best practices aimed at reducing the risk of ransomware attacks.

As cyberattacks increase, insurers focus on risky sectors

Insurers have noted for some time that the risk of malicious cyber activity aimed at the federal government, US businesses and critical infrastructure is growing. A recent 2021 report from the Government Accountability Office (GAO), released under the provisions of the National Defense Authorization Act for Fiscal Year 2021, affirms the need for a steady insurance market amid the sharp rise in cyberattacks over the past several years.

As challenges continue, insurers and policymakers are encouraged to evaluate their cyber controls, particularly within high-risk sectors. Most notably, the healthcare sector is seeking ways to protect itself as attacks rise.

Growing demand for cyber insurance policies

Among other findings, the GAO report noted a growing demand for cyber insurance policies, which is consistent with insurance price increases and more frequent and severe cyberattacks. Cyber insurance take-up rates increased between 2016 and 2020, with the highest take-up rates observed in high-risk industry sectors, among them healthcare and education. Insurance premiums, which can vary based on factors including industry, company size and cyber controls, also increased.

The report additionally indicated that insurers have reduced cyber insurance coverage limits for riskier industry sectors and that insurers are trending toward adding specific limits on ransomware coverage. According to the report, challenges that insurers and policyholders face include limited availability of historical loss and cyber event data, the risk of aggregated losses from cyberattacks and limited awareness of cyber-risks and cyber insurance coverage needed to mitigate those risks.

Cyber-risk remains high for healthcare

The analysis and accompanying trend of cyber insurance limits comes as the number of ransomware incidents has increased over the last year. Moody's Investor Services issued a report in late May that found cyber-risk remains high for the healthcare industry, noting that the growing reliance on electronic records, connected devices and digital health technology that may leave such institutions rich targets of sensitive data and susceptible to attacks.

Ransomware incidents involving healthcare and educational institutions have been rising steadily since 2019 and show no sign of declining. This summer, the FBI issued a flash bulletin warning of attacks using the ransomware Conti. *Conti* is a human-operated "double extortion" *ransomware* that steals and threatens to expose information as well as encrypting it so that its owner cannot access it. The Bureau said it had identified at least 16 such Conti attacks targeting US healthcare and first-responder networks. The FBI bulletin was made public by the American Hospital Association, which published the warning alongside a statement calling for a coordinated government campaign to disrupt ransomware organizations.

No shortage of hackers

Some ransomware organizations, such as REvil and Avaddon, have publicly committed to rules that prohibit their affiliates that use their ransomware from attacking healthcare and educational institutions. Of course, such commitments are dubious in light of the reported criminal activities of the groups and the fact that the perpetrators of these attacks may have disbanded. While perpetrators of ransomware often reemerge with new groups, there is no reason to believe they would adhere to promises made by their prior organizations to limit the scope of their operations. Moreover, there appears to be no shortage of competitors willing to target these sectors.

The GAO's findings and the recent uptick in cyberattacks and ransomware incidents demonstrate the need for cyber insurance policyholders to increase awareness about the risks and resulting costs and operational impacts of cyberattacks, particularly in such high-risk sectors as healthcare and education. Cyber insurance trends also emphasize the need for industry participants to implement and strengthen cyber controls and defenses.

Federal government offers best practices for combating ransomware attacks

In July 2021, as part of its ongoing response to the growing national security threat posed by ransomware attacks, the Departments of Justice and Homeland Security, in collaboration with federal partners, established Stopransomware.gov, a one-stop hub for ransomware resources to help private and public organizations mitigate their ransomware risk. The website offers tips and guidance to prepare for and combat ransomware attacks, and resources for reporting incidents.

Among other best practices for incident prevention, the website recommends that organizations:

(1) restrict users' permissions to install and run software applications

(2) use strong spam filters to prevent phishing emails from reaching end users

(3) authenticate inbound email to prevent email spoofing and

(4) configure firewalls to block access to known malicious IP addresses.

The website also includes a ransomware response checklist, offering best practices for incident detection, analysis, containment, and eradication.

Other cyber-risk management strategies

As the costs and sophistication of cyberattacks continue to rise, and as businesses continue to seek ways to streamline operations in response to the evolving COVID-19 pandemic, organizations should continue to monitor cyberattack trends and develop data governance programs. Other cyber-risk management strategies include reviewing organizational controls, developing and improving incident response plans, conducting internal and external security assessments, and training employees on incident prevention and response.

Reviews of recent trends and statistics provided by both public and private resources emphasize the need for organizations in high-risk industry sectors, not least healthcare and education, to recognize that expenditures for information security program development and high cyber insurance premiums with reduced limits may be part of the ongoing cost of doing business.

The advanced persistent threats of ransomware groups and other cyber criminals may pose existential threats to businesses. Investments in cybersecurity and cyber insurance are critical to businesses and may help them avoid the far higher expenses they may incur should they become victims of a serious cyberattack.

AUTHORS

Lori Marsh
Associate
Silicon Valley | T: +1 650 833 2000
lori.marsh@dlapiper.com

Emily Maus
Associate
Washington, DC | T: +1 202 799 4000
emily.maus@dlapiper.com

Anna Spencer

Partner
Atlanta | T: +1 404 736 7800
anna.spencer@dlapiper.com