Audit Insights
Helping You Succeed
ACCUITY

AUGUST 15, 2022

Cyber risks: A critical part of your auditor's risk assessment

As businesses and not-for-profit entities increasingly rely on technology, cyberthreats are becoming more sophisticated and aggressive. Auditors must factor these threats into their risk assessments. They can also help you draft cybersecurity disclosures and brainstorm ways to mitigate your risk of an attack.

Increasing risks

How much does a data breach cost? The average has reached an all-time high of $4.35 million, according to the newly released "Cost of a Data Breach Report 2022." The report, published by independent research group Ponemon Institute, also found that 83% of respondents have experienced more than one data breach.

Another key finding is that the average cost of a data breach increased by roughly 13% during the pandemic. Why? One reason is the increase in remote working arrangements. Many organizations now have sensitive data stored in more places than ever before — including laptops, cloud-based storage, email, portals, mobile devices and flash drives — providing many potential areas for unauthorized access.

Ransomware attacks are also on the rise, in part due to geopolitical instability. According to the study, ransomware attacks were up 41% in 2022 compared to the previous year. These attacks cost organizations an average of $4.54 million per incident in 2022, excluding any ransom paid to the perpetrator. Ransomware attacks generally take longer to detect and contain than other types of data breaches.

Targeted data

Hackers may try to steal valuable information about your organization's employees and customers. Examples include payment card data, protected health data and personal identifiable information, such as phone numbers, addresses and Social Security numbers.

Another target may be valuable intellectual property, such as customer lists, proprietary software, formulas, strategic business plans and financial data. These intangible assets may be sold or used by competitors to gain market share or competitive advantage.

Risk assessment

As the frequency and severity of cyberattacks have increased, data security has become a critical part of the audit risk assessment. In recent years, the Public Company Accounting Oversight Board (PCAOB) has interviewed auditors of companies that have experienced a cybersecurity breach.

These interviews reveal that audit firms provide varying levels of guidance, both when assessing risk at the start of the engagement and when uncovering a cybersecurity incident that occurred during the period under audit or during audit fieldwork. For example, auditors usually ask management what's being done to understand, detect and prevent computer system breaches.

Another key finding of the PCAOB research is that the costs associated with cybersecurity breaches may not always be apparent. A major cybersecurity breach can cause more than lost profits; it may also result in a loss of customers, reputational damage and even bankruptcy.

We can help

Though PCAOB's research focuses on public companies, any organization can be the victim of a cyberattack. And the effects may be even more devastating for those with fewer resources to absorb the losses and assign dedicated staff to respond to breaches. Our firm is atop the latest cybersecurity trends. Our auditors can help your organization assess its cyber risks and improve the effectiveness of internal controls over sensitive data. Contact us for more information.