Cybersecurity
INSIDERS

Three Risk Mitigation Strategies to Address the Latest Data Security Threats

By **Dannie Combs**

By Dannie Combs, Senior Vice President and CISO, Donnelley Financial Solutions (DFIN)

As security threats to data continue to ebb and flow (mostly flow!), I am keeping a close eye on regulations, identity and access management (IAM), and Artificial Intelligence (AI) — and I suggest that business leaders do the same. Here are three risk mitigation imperatives that can help organizations get a better handle on these latest risks and threats.

1. **Know and understand your legal and regulatory obligations.**

Organizations must understand their legal and regulatory compliance obligations. Laws and regulations around data continue to evolve, with several new bills working their way through Capitol Hill, prompting concern around enforcement, penalties, and obligations. The latest bill to address data threats is the RESTRICT Act, also known as the Restricting the Emergence of Security Threats that Risk Information and Communications Technology Act. If passed, it will significantly restrict data movement.

The bill is intended to address technology-based threats, giving the U.S. Department of Commerce power to regulate technology developed by countries that have adversarial relationships with the United States. The RESTRICT Act outlines guidelines for data sharing, encompassing a wide range of information beyond personal data; and establishes a risk-based process directed toward identifying and mitigating foreign threats to information and communications technology products and services.

2. **Assess your identity and access management framework.**

Digital identities have grown exponentially in recent years because of digital transformation, mobile adoption, online shopping, and the shift toward remote work and digital collaboration. As technology continues to advance and digital interactions multiply, the importance and prevalence of digital identities will also expand. Threats are also growing, with 40 percent of data breaches involving stolen credentials, according to the 2022 Verizon Data Breach Investigation Report. This is compelling evidence that cybercriminals are evolving their tactics and techniques — including phishing, social engineering, and malware — to exploit vulnerabilities in digital systems and gain unauthorized access to digital identities.

Robust security measures, including IAM, are needed, and here there is good news to report — more organizations are prioritizing identity and access management solutions for user accounts, privilege levels of applications, administrative roles, and even customer accounts. I recently attended Gartner’s Identity & Access Management Summit and observed a significant increase in the volume and maturity of identity management offerings.

IAM enforces the principle of least privilege (PoLP), ensuring that access to datasets is appropriately limited to only what is necessary. A strong IAM framework helps prevent unauthorized access and reduces the risk of identity compromises by providing a systematic approach to managing and controlling user identities, their access privileges, and authentication methods. Since IAM is an essential component of an organization’s cybersecurity strategy, it is important for organizations to evaluate (and reevaluate) their current IAM frameworks and ensure they are focused on identity governance administration and privileged access management technologies.

A robust IAM is also critical in industries that are subject to strict regulatory requirements concerning data privacy and security, helping organizations meet their compliance obligations by ensuring appropriate access controls, segregation of duties, and audit trails.

I have come across a helpful guide for InfoSecurity professionals that reiterates the importance of identity governance and how it gives organizations better visibility into the identities they manage: Identity and Access Management Recommended Best Practices Guide for Administrators, developed by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA). We know that better data visibility leads to better risk mitigation.

3. **Stay vigilant about security vulnerabilities in AI chatbots.**

As AI continues to rapidly evolve, integrate, and scale, organizations need to remain vigilant about its potential vulnerabilities. While platforms like ChatGPT and others offer valuable time-saving benefits, they also can introduce security risks, including intellectual property loss and automated cyberattacks.

For example, AI chatbots can be exploited to craft phishing emails, develop malicious code, or impersonate individuals, leading to ransomware attacks, cyberattacks, or fraudulent activities. There have been reports of hackers leveraging ChatGPT to generate malware and encryption scripts, which can significantly accelerate cyberattacks.

Another concern involves the exposure of sensitive data. There have been instances whereby information such as patient records, company data, or third-party information, has been input into ChatGPT, potentially posing risks if exposed at a future time. As with any game-changing technology, we can expect AI models to be regulated with safety and security standards, possibly at the government level. It is important for leaders to collectively ask: What is our AI strategy? How does AI fit into our governance model? How should we manage AI? What are our AI usage guidelines?

Improving Risk Mitigation is Achievable

Improving risk mitigation efforts may seem daunting, but it is achievable, especially when organizations have a better understanding of the cybersecurity landscape. With new security threats emerging regularly, it is essential to approach them with urgency and diligence. That’s a strategy that can greatly lower your organization’s security risk exposure and better protect your data and your organization.

cyberinsiders

No posts to display