



EBOOK

5 Data Security Trends You Must Know



5 DATA SECURITY TRENDS YOU MUST KNOW

Your data is up against a lot, and cyberattacks are just the tip of the iceberg. 94% of IT and security leaders reported their organization experienced a significant cyber attack last year.¹ Keeping that precious data safe means staying on top of emerging technologies, regulations, and even shifting priorities, so you—and your data—aren't left behind.

Let's go over five of the most important data security trends to look out for. We'll talk about how cybercriminals are using AI to make their jobs easier, how CISOs jobs are becoming more difficult, how new SEC rules will impact your attack reporting, what generative AI can do for you, and why you need to focus on cyber resilience moving forward.

1 "The State of Data Security: Measuring Your Data's Risk," Rubrik Zero Labs, 2024, <https://www.rubrik.com/zero-labs>

TREND 1

AI IS BECOMING AN INTEGRAL PART OF A HACKER'S TOOLKIT

There's a lot to be excited about when it comes to AI—but threat actors are getting in on it, too. 75% of security professionals saw attacks increase over the past year, and 85% say hackers using generative AI is fueling that growth.² Cybercriminals are using AI in new ways to gain access to your systems. Let's look at some of the ways AI is making attackers' jobs easier.

Phishing is one area where AI is especially helpful for criminals. SlashNext found a 1,265% increase in phishing emails using AI tools.³ AI can create convincing fake emails or websites, making it harder for victims to distinguish fact from fiction.

Another way hackers are gaining access to systems is through password cracking. Certain AI programs can crack common passwords, with Home Security Heroes finding that one tool can hack over half of the most commonly used passwords in under a minute.⁴ Gaining access to passwords means hackers can just log in to your systems, making it even harder to know you've been breached.

And these criminals aren't just using AI to get in to systems. They're also using it to automate various hacking activities, like testing for vulnerabilities they can exploit during their attack. This means they can escalate their attacks sooner and make them even more devastating.

2 "Study finds increase in cybersecurity attacks fueled by generative AI," Security Magazine, <https://www.securitymagazine.com/articles/99832-study-finds-increase-in-cybersecurity-attacks-fueled-by-generative-ai>

3 "The State of Phishing 2023," SlashNext, n.d., <https://slashnext.com/state-of-phishing-2023/>

4 "An AI Just Cracked Your Password," Home Security Heroes, 2023, <https://www.homesecurityheroes.com/ai-password-cracking/>

TREND 2

CISOS' JOBS AREN'T GETTING ANY EASIER

CISOs already have a lot on their plate—and that's not expected to change any time soon. In the next section, we'll talk about how new regulations are contributing to a CISO's responsibilities, but for now, what you need to know is that the Securities and Exchange Commission (SEC) has passed rules requiring companies to disclose when they've faced a material breach.

The other thing CISOs need to prepare for is just how much time they'll be spending dealing with ransomware. A recent study by Sophos found that it's taking organizations longer than ever to recover, with over a third needing over a month.⁵

Ransomware isn't letting up

Ransomware in 2023 was 70% higher in volume than in 2022, with a total of 4,399 publicly reported ransomware events.¹

Once an attack has been launched, finding out what data has been affected isn't cut-and-dry. Hackers will often stay in hiding for weeks, using that time to identify what sensitive data an organization has, so their attacks hit even harder.

To put even more pressure on CISOs' shoulders, ransomware actors are increasingly demanding a second ransom to prevent a data leak. And these days, double, triple, and even quadruple extortion are not unheard of. But these harsher threats aren't being matched with more fine-tuned cybersecurity skills. CISOs are having a tough time finding skilled cybersecurity professionals to keep their environments safe.

5 "The State of Ransomware 2024," Sophos, 2024, <https://www.sophos.com/en-us/content/state-of-ransomware>

TREND 3

NEW SEC RULES ARE CHANGING WHAT COMPANIES HAVE TO SAY ABOUT CYBER INCIDENTS

The Securities and Exchange Commission (SEC) recently released new rules that require public companies to disclose material security incidents on Form 8-K. The ways a company decides if an incident counts as “material” are varied, but things like the probability of harm, the severity of the loss, and the impact on a company’s reputation certainly count.⁶

Here’s how it works: Companies have 4 business days from an attack to describe the incident and the impact—including what data was affected and when. Companies also need to share what cybersecurity technologies they’re using to try to thwart attacks and what damage could come if threat actors can get around those technologies.

While these new rules are stressful enough, adversaries are putting additional pressure on their victims to respond to their ransomware threats by reporting these companies to the SEC.

For CISOs, these new rules will make their jobs even harder. In October 2023, the SEC filed a lawsuit against a company and its CISO for fraud, claiming they had misled investors about their cybersecurity practices. Moving forward, CISOs will need to be more diligent than ever about their companies’ cyber preparedness.

6 “SEC Issues New Requirements for Cybersecurity Disclosures,” Deloitte, July 30, 2023, <https://dart.deloitte.com/USDART/home/publications/deloitte/heads-up/2023/sec-rule-cyber-disclosures>

TREND 4

GENERATIVE AI CAN LEVEL THE PLAYING FIELD BETWEEN HACKERS AND CISOS

We've mentioned AI in an earlier section, but generative AI is in a category all on its own for its potential to shift the tides in the battle between cyberattackers and CISOs.

While the speed and sophistication of attacks are on the rise because of generative AI, CISOs are also leveraging generative AI to level the playing field. IBM found that AI and automation saved organizations about \$1.8 billion in data breach costs and helped organizations identify and contain threats 100 days faster.⁷

If we look at a ransomware attack, for example, recovery can sometimes take weeks or months. Organizations often need a lot of time to figure out how the attack happened, what was affected, and how to get their data back. They also need to make sure all traces of the attack are eradicated, so they don't reinfect their systems with any leftover malware.

Generative AI helps organizations respond much faster, so they can get back to business sooner. Ruby, a recently launched generative AI companion to Rubrik Security Cloud, makes recovery faster by providing step-by-step guidance on how to recover—and it's so simple that you don't even need to be an expert to understand them.⁸

The true cost of cybercrime

93% of organizations that endured a successful ransomware attack reported paying a ransom demand with 58% of these payments motivated by threats to leak stolen data.¹

⁷ "Cost of a Data Breach Report 2023," IBM, 2024, <https://www.ibm.com/reports/data-breach>

⁸ "Ruby, the Generative AI Companion for Rubrik Security Cloud," n.d., Rubrik. <https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/brf-ruby-the-generative-ai-companion-for-rsc.pdf>

TREND 5

ORGANIZATIONS NEED TO FOCUS ON CYBER RESILIENCE, NOT JUST PREVENTION

Let's cut to the chase: Cyberattacks are inevitable, and the stakes are material. One of every two organizations suffered a loss of sensitive data last year.⁹

But the ripple effects of an attack don't just affect an organization's data. One company that faced a ransomware attack last summer said the incident contributed to a 4% drop in its first-quarter revenue, and another company hit in the fall suffered a \$100 million loss.

The consequences are dire, but many organizations still hold onto a "it won't happen to us, or won't happen anytime soon" optimism bias that keeps them from being truly prepared to survive an attack.

You need to accept the fact that breaches will happen. Instead of focusing solely on prevention, you need to make cyber resilience a priority. Cyber resilience goes beyond prevention, putting the focus on bouncing back from an attack using a two-phased approach.

The first part is about understanding where corporate data lives, how sensitive that data is, and who has access to it. The second part involves ensuring that data is secure and available, so you can restore your files and workflows quickly after an attack. When organizations know where their data is and can recover that data, they can get ahead of the financial damage an attack can cause and speed up their response times.

⁹ Rubrik Zero Labs. "The State of Data Security: The Journey to Secure an Uncertain Future," n.d., Rubrik. <https://www.rubrik.com/zero-labs>.

WHERE DO WE GO FROM HERE?

A breach doesn't have to mean the downfall of your data, your reputation, or your organization. You need to come up with a “bounce back” plan that makes sure your organization comes out of the next attack practically unscathed—while staying in compliance with new SEC requirements.

Rubrik is in the business of helping organizations come back from attacks stronger. To find out how we've helped thousands of your peers do the same, [click here](#).

