Ransomware Costs Businesses Record-High $1 Billion in 2023: Your 5-Step Plan to Prevent Attacks in 2024

Insights
2.21.24

2023 was the most devastating year yet for ransomware attacks, with businesses forking over $1 billion in ransom payments for the first time ever – and 2024 is expected to be even worse. Beyond the payments, the average cost of each ransomware attack last year was over $5 million. Given these unprecedented statistics, ransomware attacks could be the largest, looming threat to your business in 2024. This Insight provides a clear five-step plan to help you lower the odds of falling prey to a costly attack.

The Basics

- Ransomware is malicious software that blocks access to computer systems or files until you pay a sum of money to the cybercriminals who have infiltrated your business. They gain access by exploiting system vulnerabilities (sometimes through a third-party or vendor that has access to your system) or by luring your employees into clicking on links or attachments or responding to phishing emails or "smishing" texts (phishing through SMS texts).
- The $1.1 billion tally of ransoms paid in 2023 was particularly shocking because it nearly doubled the $567 million in ransoms paid out in 2022.
- Not including the payouts, the average cost of a ransomware attack – including detection and escalation, notification, post-breach response, and lost business – rose to $5.13 million in 2023, which represents a 13% increase from 2022.
- Federal and International Law enforcement have deployed extensive efforts to minimize ransomware attacks on a global scale. Just days ago, in fact, the FBI and UK National Crime Agency made headlines as they implemented "Operation Cronos" and disrupted one of the world's most potent ransomware attackers.
- Despite law enforcement's efforts to smother these cyber threats, experts project an increase in cyber syndicates in 2024. Allan Liska, Threat Intelligence Analyst at cybersecurity firm Recorded Future, commented, "A major thing we're seeing is the astronomical growth in the number of threat actors carrying out ransomware attacks." Recorded Future reported 538 new ransomware variants in 2023.

5-Step Plan for Businesses to Prevent Costly Ransomware Attacks in 2024

1. Provide Updated Cybersecurity Training

You should provide updated and robust cybersecurity training to all your employees (including very busy executives) on an annual basis. According to the 2023 Cost of Data Breach report (CODBR), phishing and compromised credentials were the most common initial attack vector for data breaches, demonstrating that threat actors still count on a shortfall in employee oversight to gain access to valuable, confidential data.

The latest data from the CODBR also suggests that cybersecurity training is a wise investment for employers. In 2023, organizations with a high level of employee training that suffered a data breach incurred a significantly lower than average cost in managing and responding to the data breach incident – on average, data breaches cost $770,000 less for organizations with high level of employee training and $640,000 more for organizations with low levels of employee training.

This data underscores the importance of ensuring that all employees with access to sensitive data are familiar with the basic principles of data security. Make sure to train them to understand the red flags that will help them detect phishing emails and other common tactics used to compromise credentials.

2. Maintain and Test Your Incident Response Plan

Create, maintain, and exercise a data security incident response plan (which addresses all data security incidents, not just those rising to the level of a reportable data breach under applicable law), resiliency plan, and associated communications plan. The response plan should include response and notification procedures for ransomware incidents. You should also ensure that your incident response plan is regularly tested and updated, as cyberthreats are quickly evolving. Engage in what is called a "table-top exercise" at least annually, which is like a fire drill but for data security.

According to the 2023 CODBR, employers who maintained an incident response team and plan were able to identify and contain data breaches an average of 54 days (19.4%) faster than employers who did not maintain an incident response strategy. Lower identification and containment times provably lowers the cost of a potential breach, as breaches with identification and containment times under 200 days cost organizations 23% less in 2023 than organizations who took longer to identify and contain data breaches.

3. Implement Artificial Intelligence or Automated Cybersecurity

As ransomware gangs continue to rely on new strains of malware and other new technologies to infiltrate valuable data, you should familiarize yourself with the latest defense and detection technologies to develop more proactive cybersecurity systems.

For example, using artificial intelligence (AI) and automation across cybersecurity threat detection and response tools can help analysts detect new threats faster and more accurately than ever before. These technologies have already proven effective for employers who fell victim to data breaches in 2023. In fact, the 2023 CODBR found that employers that extensively used AI or automated cybersecurity systems saved nearly $1.8 million in data breach costs and enjoyed accelerated data breach identification by over 100 days, on average.

4. Secure and Encrypt Data Stored in the Cloud

Due to the increased number of remote workers, many employers have implemented cloud-based storage and systems into the workplace over the past several years. Given this rise in popularity, threat actors have consistently targeted these stockpiles of valuable data, including employee and consumer personally identifiable information (PII). In 2023, in fact, 82% of all data breaches involved cloud-based data, and these breaches involved higher costs and longer identification and containment time.

To reduce risk, you should require multifactor authentication for employees to gain access to company networks. You should also create and maintain secure, offline, and encrypted backups of your data, and regularly test those backups. Moreover, you should choose strong cloud providers that adhere to strict security protocols and standards, such as the implementation of DevSpecOps application development.

5. Engage Counsel to Ensure Regulatory Compliance

Businesses across the country continue to face increased data privacy requirements thanks to a wave of new laws cropping up state by state. For example, The U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) may impose federal sanctions on companies that facilitate ransomware payments to a sanctioned person, even if the ransomware victim was unaware of the sanction nexus. Failure to comply with such regulations proved costly for employers impacted by data breaches in 2023.

According to the 2023 CODBR, organizations with low levels of regulatory compliance suffered an average cost of $5.05 million per data breach, a whopping $1.04 million more than organizations with high levels of regulatory compliance.

Fortunately, you can easily avoid this unnecessary cost by engaging knowledgeable counsel before a breach occurs to not only ensure compliance with data privacy regulations but to put yourself in the best position to minimize such threats.

Conclusion

Fisher Phillips will continue to monitor further developments in this area, so be sure to subscribe to Fisher Phillips' Insight system to stay up-to-date. If you have any questions regarding how

cybersecurity threats could impact your organization, or best practices for addressing those threats, please consult your Fisher Phillips attorney, the authors of this Insight, or a member of Fisher Phillips' Privacy and Cyber Practice Group.

Related People

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Andreas Moghimi
Associate
213.402.9586
Email

Service Focus

Privacy and Cyber