# Ransomware in 2024: Last Year's Lessons Inform Today's Strategies

Just over one year ago, experts suggested that ransomware attacks had begun to decline. But then 2023 got underway and blew that theory out of the water. In fact, according to Malwarebytes, ransomware attacks in 2023 soared 70 percent higher than 2022. Ransomware in 2024 promises more pain, but last year's lessons help guide proactive security strategies.

## Not Your Momma's Ransomware

Threat actors still overwhelmingly use phishing emails to launch their attacks. And they continue to exploit known vulnerabilities on unpatched systems. Some things never change. But the nature of these attacks constantly evolves. Like studying the opposing team's game plays, understanding current trends can help organizations shape their defense.

In the first place, we have seen ransomware gangs increasingly turn their attention to supply chain attacks. For instance, in May 2023, a Russian gang exploited a zero-day vulnerability in MOVEit, a file transfer platform used by thousands of organizations around the world. The attack affected over 2500 organizations and 67 million people.

In a related development, threat actors have upped their attacks against high-value or high-profile organizations. This big-game hunting targets companies with treasure troves of sensitive data, strict compliance requirements, and complex systems. With so much at stake, the organizations are more likely to pay.

Next, enter double and triple extortion schemes. In the old days, attackers entered the system, encrypted information, and demanded a ransom. Now they both encrypt data and exfiltrate data to an external location. Finally, they demand payment for a decryption key, as well as for not leaking the information.

Experts have also noted a rise in "follow-on" extortion attacks. In these attacks, fake "security researchers" contact ransomware victims and offer assistance in exchange for Bitcoin payments.

## And to Complicate Matters Even More…

Several factors make these evolving ransomware attacks particularly difficult to prevent and address. For instance, ransomware-as-a-service (RaaS) and AI have streamlined the process and made it easier for even less experienced criminals to launch successful attacks.

In addition, 5G networks have given rise to vast numbers of connected devices, with over half the world's data projected to come from IoT devices by 2025. While this represents a boon for industry, every IoT device adds another possible entry point for hackers. Similarly, frequently lax security on mobile devices exposes both personal and business data to attack.

Finally, the cyber security skills gap continues to grow. Currently, the gap stands at 3 million people. Organizations simply do not have the security personnel they need to protect against growing threats.

## Update Cyber Security to Protect Against Ransomware in 2024

Responding to evolving ransomware threats, the Cybersecurity and Infrastructure Security Agency (CISA) has released updated guidelines that include the following:

- **Limit use of remote desktop services** – Threat actors frequently gain access to the target system through poorly-secured remote services. Once they have initial access, they use native Windows RDP client to move through the network.
- **Update security awareness training** – Effective employee training must include teaching users how to recognize signs of advanced social engineering. Phishing simulations will help to cement this knowledge.
- **Segment networks** – By separating the network into distinct, contained parts, security teams make it difficult for attackers to move through the system. Minimize users and resources with access to each segment, following the principle of least privilege.
- **Strengthen and enforce MFA** – Where possible, implement multi-factor authentication (MFA). Keep in mind that not all MFA methods offer the same protection. For instance, biometric authentication and phishing-resistant MFA offer more protection than a code sent to a mobile device.

- **Implement a zero-trust architecture** – This access management strategy involves requiring identity verification any time a user, application, or device requests system access.
- **Prioritize patching to address known exploited vulnerabilities** – In several high-profile attacks in 2023, threat actors successfully targeted known vulnerabilities in unpatched systems. Prioritize patch management.
- **Deploy EDR solutions to protect endpoints** – At some point, every organization will find themselves in the ransomware crosshairs. Endpoint detection and response (EDR) solutions work to identify and remove threats early—before they escalate.

- **Revisit your backup strategy** – It seems to me that no ransomware protection strategy would be complete without a reminder to update and test your backup strategies. When ransomware hits, having a recent backup speeds recovery and reduces downtime.

## Bring Security Experts to the Table

With a widening cyber security skills gap, many organizations find these security recommendations overwhelming. But even small businesses can tap into enterprise-grade cyber security by partnering with a managed services provider such as eMazzanti Technologies. Our security experts will tailor a comprehensive solution to your specific environment and budget.