Protecting Your Organization from Cyber Attacks

Google 'what are the major cyber-attacks in 2024.' The list is astounding and the tip of the iceberg as these are only some of the reported attacks.

The good news is that most attacks are stopped before damage occurs. The bad news:

- Cyber-attacks have doubled between 2016 and 2022.[1]
- According to Statista, there were 73% more data breaches in 2023 than in 2021.[2]
- A recent Sophos survey reported that the average ransomware payout doubled from $812,000 in 2022 to $1.54 million in 2023.[3]

One common misperception about cyber-crime is that threat actors target large organizations exclusively. Unfortunately for small-to-medium sized organizations, this is not the case. *As ransomware attacks have increased over the past two years, threat actors have turned more to trawling smaller companies than 'whaling' after larger enterprises.*[4]

"Threat actors know smaller organizations have vulnerabilities. They lack the budget for every commercially available cyber control," says Jason Rebholz, Chief Information Security Officer for Corvus Insurance. *"At the end of the day, threat actors are after a payday, no matter who pays."*

THREAT ACTORS ARE OPPORTUNISTIC, TARGETING ANY ORGANIZATION NO MATTER THEIR SIZE.

- 47% of overall cyber claims impacted organizations in the $0–$100M revenue band.
- 67% of overall cyber claims impacted organizations in the $0–$200M revenue band.
- 50% of ransomware-related claims impacted organizations in the $0-$200M revenue band.

Source: Corvus claims data.[5]

ORGANIZATIONS NEED CYBER RISK CONTROLS AND CYBER INSURANCE

Implementing a cyber risk management program is now table stakes for organizations, no matter their size. Doing so is critical for their protection and obtaining cyber insurance.

Cyber carriers have evolved their view on the need for cyber controls. *"Carriers are looking for a set of standard controls to make sure companies are doing at least the bare minimum to protect themselves,"* says Rebholz.

In today's risk environment, cyber insurance complements cyber controls. Together, they build a defense to protect organizations from cyber events, and a financial backstop with respect to the losses — including business downtime and reputational harm, that such an event can cause.

CYBER RISK MANAGEMENT

There are four ways organizations can take on risk:

Acceptance

Avoidance

Reduction

Transfer

"Of course, the top priority is to avoid risk," says Daniel Ahmed, Corvus Insurance Senior Cyber Security Advisor. *"Cyber insurance is necessary to help mitigate the 'worst-case scenario,' but organizations must still manage the day-to-day security program."*

Rebholz compares cyber insurance to healthcare insurance. *"You have health insurance to pay for both routine and unexpected costs, but you still take care of yourself in order to prevent unnecessary doctor and hospital visits."*

THREE BUCKETS OF CYBER RISK MANAGEMENT:

Protecting the environment

Create a risk management program that hampers or avoids attacks from an organization level to a personnel level.

Detection and response

Organizations should assume that a data breach or cyber attack is possible and develop protocols to detect the breach or the type of attack and where it is focused. Organizations should then create a plan to contain the incident to limit the damage.

Organizational resilience

Ensure your organization is prepared for system and data failure with backups and offline copies to minimize downtime.

TAKE A LONG-TERM APPROACH

William Boeck, IMA Executive Vice President and Cyber Product Leader, encourages organizations to start with the basics. *One of the easiest — and most effective — controls to implement is multi-factor authentication (MFA).* According to Corvus statistics, **85% of ransomware claims by organizations with revenues less than $100M could have been prevented if MFA was properly enabled and enforced.** Many out-of-the-box SaaS applications, such as Microsoft 365 and Google Suite, offer MFA as part of the package.

Email protection is another must-have. This control provides a base level of protection by detecting and preventing basic email-borne threats such as spam and spoofed emails. Like MFA, email protection comes standard in M365 and GSuite, and among other SaaS apps. Enabling and enforcing this tool along with MFA starts to build a strong shield of defense, especially against phishing email attacks — a favorite weapon threat actors use.

According to Rebholz, these applications are becoming table-stakes if organizations want to ensure cyber insurance coverage, or renewals. *"Cyber carriers are looking for a set of standard controls, to make sure companies are doing the bare minimum to protect themselves."*

Boeck also encourages companies to implement a back-up strategy. In the event of a breach, organizations can minimize downtime by duplicating of every file, all data, applications, and protocols. Boeck points out that it is critical the back-up system is completely segregated from the main environment: *"If your back-ups are connected to the production level that is infected, locked out, or offline, the back-ups are too."*

CYBER SECURITY RISK MANAGEMENT CONTROLS — BASICS TO ADDITIONAL TOOLS:

CONTROL	WHERE TO START	WHERE TO INVEST
MFA (must have)	Free MFA applications *(Microsoft Authenticator or Google Authenticator)* for remote access and external email access	SSO *(single sign-on)* for business-critical applications and Passkeys for admin accounts
Email Protection (must have)	Built-in email filtering *(M365 and Google Workspace)*	Advanced *Secure Email Gateways* to block advanced email threat
Backups (critical to have)	Offline or Airgapped Backup Copy	Immutable Backup Copy to avoid intentional deletion
Endpoint Protection	Endpoint Detection and Response (EDR) *(baseline protection and automated threat response)*	Managed Detection and Response (MDR) *(outsourced full stack 24/7/365 monitoring)*
Identity Verification	Multi-factor Identification	Out-of-band authentication (OOBA)

SECURITY IS A JOURNEY

It isn't realistic for every organization to implement every control right away. There are costs involved that make some controls out of reach to organizations with limited budgets and staff. *"To get the most bang for their buck, organizations need to understand what security means to them,"* says Ahmed.

Budget season is the right time for organizations to develop near-term and long-term cyber-security strategies. Organizations need to understand the threat landscape particular to them, to their industry and to the regions they operate. After undergoing an in-depth threat analysis, organizations can prioritize where to tackle the gaps in their defense and then look to strengthen their long-term defenses.

Undertaking a threat analysis can be an overwhelming project for organizations. Relying on a trusted partner for guidance is an opportunity to lean on their experience and perspective. Cyber insurance carriers often offer services that organizations can use for consultations on everything from assessment to vendor and management recommendations. Rebholz estimates the services that Corvus offers can be worth up to $80K a year for clients.

CONTRIBUTORS:

- **Tim Burke,** *Executive Vice President, Cyber/Commercial Client Advantage*
- **William Boeck,** *Executive Vice President, Cyber Product Leader Client Advantage*
- **Jason Rebholz,** *Chief Information Security Officer, Corvus Insurance*
- **Daniel Ahmed,** *Senior Cybersecurity Advisor, Corvus Insurance*
- **Angela Thompson,** *Senior Marketing Specialist, Market Intelligence & Insights*
- **Brian Spinner,** *Senior Marketing Coordinator, Market Intelligence & Insights*

SOURCES:

1. Petrosyan, Ani (2024, August 20). *Annual number of cyberattacks in the United States from 2016 to 2022*. Statista. https://www.statista.com/forecasts/1448523/us-cyberattacks-annual#:~:text=In%202022%2C%20around%20480%2C000%20incidents,uptick%20in%202020%2C%20reaching%20540%2C000.
2. Petrosyan, Ani (2024, February 12). *Number of data compromises and impacted individuals in U.S. 2005-2023.* Statista.com. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
3. Thomas, Daniel. (2023, August 7). *Report: Ransomware payouts and recovery costs went way up in 2023.* SC Media. https://www.scworld.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023.
4. Townsend, Kevin. (2024, August 7). *Ransomware in 2024: More Attacks, More Leaks, and Increased Sophistication.* Security Week. https://www.securityweek.com/ransomware-in-2024-more-attacks-more-leaks-and-increased-sophistication/.
5. Rebholz, Jason, and Ahmed, Daniel. (2024, September). Interview with Corvus cyber experts.