CONVERGE
TECHNOLOGY SOLUTIONS

Executive Briefing

Cybersecurity Threat Report Analysis 2024

Daniel Gregory
Director | Security Architecture

Overview

In an era where cyber threats evolve with alarming speed and complexity, staying ahead requires more than just vigilance—it demands strategic insight and advanced preparedness. This executive briefing distills critical insights from several of the annual global threat reports, pinpointing the top cybersecurity challenges and opportunities most organizations face today. Designed to provoke thought and action, it aims to equip you with an understanding of emerging threats, from the rise of generative AI in cyber attacks to the intricacies of third-party risk management. Our objective is to catalyze robust discussions on enhancing your cybersecurity posture by leveraging Converge's service and solution expertise. This document is your guide to forging a more secure, resilient future in a landscape marked by increasingly sophisticated cyber adversaries.

As a world-class cybersecurity services organization, Converge maintains a close-knit, collaborative relationship with a host of top-tier vendors as well as several industry-recognized thought leaders, ensuring a deep understanding of the threat and risk management landscape. We recognize you may encounter challenges in extracting and applying the critical insights from extensive global threat reports to your unique organizational context, and the question of "***What next?***" often looms large post-analysis.

Converge has distilled the reports into eight key takeaways, each accompanied by a trio of incisive questions crafted to evaluate your organization's cybersecurity readiness and propel you towards actionable next steps.

Aiding your cybersecurity vigilance is very important to us. We invite you to engage with these takeaways and utilize the questions as a springboard for fortifying your defenses. Should you wish to delve deeper or seek guidance on implementing advanced security strategies, our experts at Converge are at your disposal.

Let's proactively shape your cybersecurity landscape.

Request My Meeting

1. Increased Use of Generative AI by Adversaries

How is your organization staying ahead of AI-powered threats, and do you have specific defenses in place against AI-generated phishing or social engineering attacks?

Given the potential for adversaries to leverage generative AI in crafting sophisticated attack vectors, what measures are you taking to ensure that your detection and response capabilities can keep pace?

Are you incorporating any form of AI or machine learning in your cybersecurity operations to counteract the rise of AI-assisted threats, and how do you plan to evaluate their effectiveness?

2. Rise in Identity-Based and Social Engineering Attacks

With the increasing prevalence of identity-based attacks, how confident are you in your current identity and access management solutions to prevent unauthorized access?

How would you rank your organization's current process for training employees to recognize and respond to social engineering threats, especially in remote or hybrid work environments?

Given the advancements in techniques used to bypass security measures like MFA, what additional layers of security are you considering or have implemented to protect user identities?

3. Cloud Environments Targeted by Adversaries

As cloud environments are targeted more by adversaries, what specific cloud security strategies have you implemented to protect your infrastructure and data?

How often do you review and update your cloud security policies and configurations to ensure alignment with the latest threat intelligence and best practices?

Could you describe how your incident response plan addresses potential cloud environment breaches and how frequently the plan is tested?

4. Supply Chain Attacks

In light of the increased focus on supply chain attacks, how does your organization assess the security posture of its suppliers and partners?

What steps have you taken to mitigate the risk of a supply chain attack impacting your operations, including any changes to vendor management or procurement processes?

How would you describe your level of visibility into the security practices of your third-party vendors, and how do you ensure continuous compliance with your security standards?

5. Increased Exploitation of Vulnerabilities

How effectively does you current vulnerability management program identify and prioritize patching, especially for zero-day vulnerabilities and critical systems?

What measures do you have in place to detect anomalous activities that could indicate the exploitation of a previously unknown vulnerability?

Are you conducting regular penetration tests and red team exercises to simulate real-world attacks and assess the resilience of your defenses against vulnerability exploits?

6. Rise in Ransomware and Extortion Attacks

Do you have a comprehensive incident response plan specifically for ransomware attacks, and how often is this plan tested with tabletop exercises?

What strategies are in place to ensure the integrity and accessibility of your backups, and are they isolated from your main network to prevent simultaneous compromise?

How are you leveraging threat intelligence to stay ahead of emerging ransomware tactics and indicators of compromise (IoCs) that could impact your organization?

7. Human Element in Breaches

How are you measuring the effectiveness of your security awareness training, and are there metrics in place to track improvements in employee behavior over time?

What additional layers of security (e.g., MFA, least privilege) are you implementing to mitigate the risk of human error leading to a security breach?

How often do you reassess the access rights of employees to ensure they are commensurate with their job roles, particularly after role changes or departures?

8. Financially Motivated Attacks

Considering the high prevalence of financially motivated attacks, how do you ensure that your protective measures to align with the most likely financial threats?

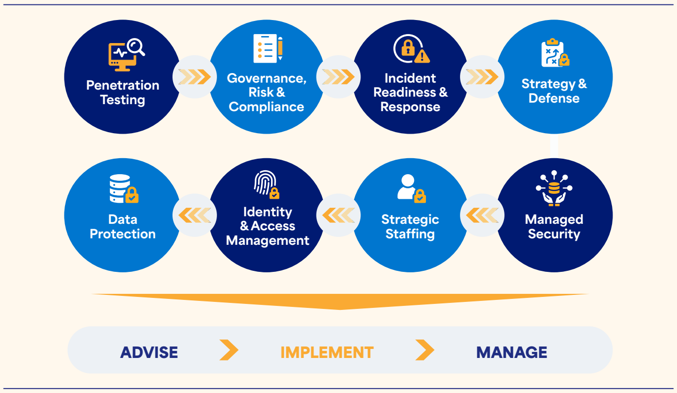
What specific controls and monitoring capabilities do you have in place to detect and respond to business email compromise (BEC) and other financial fraud tactics?

How are you engaging with industry peers and law enforcement to share information about threat actors and their evolving tactics to better protect your financial assets?

Relentlessly Focused on Cybersecurity

When you partner with Converge Cybersecurity, you can expect your priorities to be ours. Our team of strategists, former CISOs, and security experts provide unbiased expertise to help you build, manage, and optimize cybersecurity across your enterprise.

From technology solutions to advisory services, we bring our decades on the front lines of cybersecurity to help you safeguard your organization in a shifting landscape of risks, vulnerabilities, and regulations. We listen first, apply our expertise to address your challenges, and ensure that the technologies we deliver meet your current and future needs.



Penetration Testing

Governance, Risk & Compliance

Incident Readiness & Response

Strategy & Defense

Managed Security

Strategic Staffing

Identity & Access Management

Data Protection

ADVISE

IMPLEMENT

MANAGE

Converge Technology Solutions is a services-led, software-enabled, IT & cloud solutions provider focused on delivering industry leading solutions and services.