JUNE 2025

BRC
BOARD RISK COMMITTEE

BOOZ ALLEN
Cybersecurity Article

MOVING FROM RESPONSE TO RESILIENCE

How Boards Can Help Executive and Technical Leadership Navigate Cybersecurity Incidents with Confidence

By Caroline McGlynn, Esq. and Jennifer Polliard

From ransomware and supply chain attacks to global data breaches of personal information, cyber attacks are increasing—and so is their media coverage. With rising risk and growing public awareness, there's mounting pressure on businesses to do more to protect data from cyber criminals and nation-state adversaries.

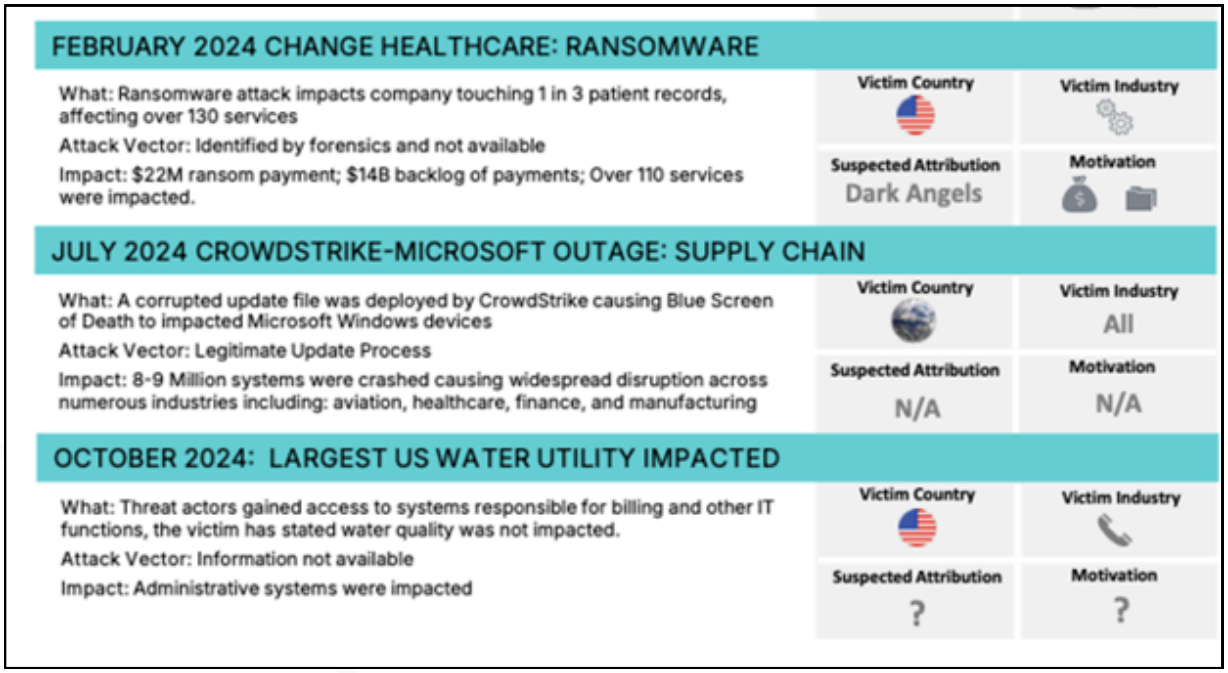

Figure 1. Recent cyberattack headlines.

Fostering a Proactive Cybersecurity Posture

Defending enterprises against cyberthreats is a business imperative. The vulnerabilities listed in the figure below are only a snapshot of the kinds of sophisticated, large-scale cyberattacks Booz Allen tracks on a daily basis for our clients.

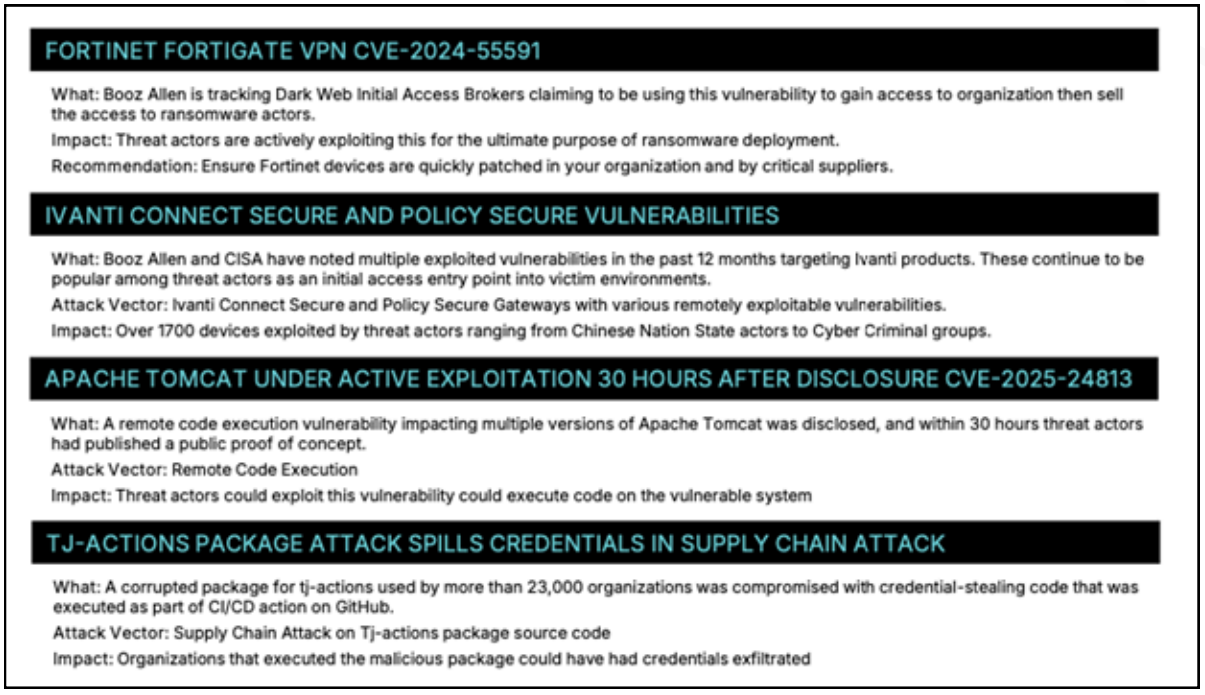

Figure 2. Notable vulnerabilities

Unfortunately, cybersecurity can get sidelined amid competing priorities. Security leaders must balance budget constraints, personnel requirements, and the challenge of aligning technical and executive leadership on actual versus perceived risk.

It's often easier to see the value of defensive strategies in hindsight. Technical leaders may find themselves transitioning from requesting resources and justifying changes to defending why changes weren't made sooner.

That's why businesses should foster an executive culture that sees, understands, and supports the need for continuous evaluation and improvement of cyber defense strategies. A successful defense-in-depth strategy depends on executive-level awareness of the risks the enterprise takes on by failing to act.

How Boards Can Help

Executive leaders must not only support the need for proactive cyber defense strategies but also empower technology leaders to execute against them. This is where board leadership comes in. Through accountability and organizational priority setting, boards can help align executive leaders and foster an environment that prioritizes proactive action over defensive strategies. This action-oriented alignment helps organizations with two business imperatives:

1

Withstand Regulatory Scrutiny

Executive-level alignment and technical leader empowerment are key to enterprise preparedness for increased regulatory scrutiny. Debriefs accompanying recent SEC rules emphasize corporate accountability by comparing the severity of cyber breaches to material losses, like a factory closing due to a fire. To demonstrate cybersecurity and withstand regulatory inquiry, businesses must design and document processes and procedures for the following domains:

- incident report cadence,
- method used to generate reports, and
- impacts on critical infrastructure

Companies must also show how their policies and procedures safeguard consumers' right to privacy or, depending on scale, the health and safety of global citizens.

2

Avoid Common Missteps

Insufficient decision authority is one of the leading reasons that Recovery and Remediation (R&R) gets delayed. For example, two of the most common missteps in ransomware negotiations are:

- a lack of executive-level exposure and
- CISOs and technical leaders who are not sufficiently informed or empowered.

CISOs recognize the dangers cyberthreats pose and understand the potential business impacts. Supported by the board, executive leadership needs to empower technical leaders to proactively address security gaps.

Figure 3. Recovery & Remediation (R&R)

How An Independent Perspective Can Help

Companies need independent investigations into the root cause, data staging, and access to or exfil of data. This information can shed light on how a cybersecurity incident happened, who was affected, and how it impacts the enterprise. But the benefit of engaging an independent investigator extends beyond information finding. An experienced independent investigator can:

- provide visibility into the incident through an independent corporate governance lens.
- translate operational impact and technical investigative findings into short- and long-term roadmaps, enabling the organization to achieve resilience long after the investigation concludes.
- work closely with C-level executives to translate technical information and develop a reporting structure on incidents, helping foster a culture of cybersecurity awareness that's critical before, during, and after incidents.
- prepare the enterprise for increased regulatory scrutiny.
- coach and prepare leadership for congressional testimonies and provide detailed reports for regulator briefings.
- answer regulator questions and requests.

CASE STUDY

Criminal Ransomware Actor Target: Global Commercial Enterprise

This real-world example demonstrates how Booz Allen supported a global commercial enterprise client after the incident had occurred. It underscores the importance of proactively investing in security programs to prevent a breach at this scale.

Identifying The Incident: Endpoint detection and response (EDR) alerts indicated unusual activities. A subsequent SOC investigation uncovered further suspicious actions.

Anomalous Activities Noted:

- Pass-the-hash attacks
- Lateral movement through several administrator accounts
- Encoded PowerShell commands enough unprotected systems to
- Unauthorized admin account activities

Why This Occurred:
Years of security program neglect allowed the threat actor (TA) to exploit a misconfiguration, find enough unprotected systems to escalate privileges to a domain level, and remain hidden long enough to steal valuable data.

Company Strengths:

- The company regularly conducted Tabletop exercises.
- They invested in top-tier security tools.
- They maintained an around-the-clock SOC staffed by skilled, vigilant analysts.

Company Challenges:

- Reduced focus on security over time due to market shifts, new acquisitions, business realignments, and evolving leadership priorities.
- Diminished CISO budget and authority.
- Modernization plans cut from the budget leaving legacy systems in place.
- Inadequate audit and review processes due to under-funding and under-staffing.

Booz Allen Engagement:

- Incident response
- Forensic analysis
- TA communications
- Dark web surveillance
- Rapid containment

Containment:

- Our analysts *reconfigured the EDR system to block malicious activity* as opposed to merely monitoring and reporting,
- i*dentified network visibility gaps and addressed them* through additional EDR agent deployment,
- *enhanced visibility, and*
- *implemented several containment strategies* including network segmentation, VPN disconnection, password changes, MFA enforcement, identifying and deactivating compromised accounts, and blocking backdoors and other TA indicators of compromise.

Post Containment:

- Investigated to identify the criminal ransomware TA.
- Found proof of extensive data theft and ransomware staging indicating imminent encryption.

The Outcome:
The company averted a catastrophic production network shutdown thanks to swift action by the company's SOC, immediate execution of the response plan, expert intervention, and decisive containment measures by company leadership. However, while they avoided encryption, the company did face public backlash, data exposure, stock volatility, and breach reporting. Like many firms facing a major cyber breach, this business heavily invested in its security program post-breach to prevent a recurrence. These accelerated efforts led to significant expenditures and had severe budgetary impacts, whereas more proactive measures would have been less expensive and may have helped prevent a breach at this scale.

Leadership Alignment Builds Resilience. And It Starts With the Board.

Cyberthreats pose business risks that demand attention from the highest levels of leadership. Building organizational resilience requires more than sophisticated technical solutions: it depends on aligned leadership, clear decision authority, and sustained executive support. The board plays a critical role in prioritizing investment, setting expectations, and reinforcing accountability. By fostering a culture of preparedness and supporting proactive defense strategies, boards can help ensure the enterprise is prepared to navigate an evolving threat landscape with confidence.

Looking for a place to start the conversation with executive leaders at the organization you govern? This list merges the Incident Response team’s recent observations with insights from across the cybersecurity community. It offers detailed, actionable insights to improve cybersecurity against emerging threats.

The information shared here is intended to provide a snapshot of current activity and is subject to change as the various threat group tactics, techniques, and procedures evolve.

Device, Appliance, OS, Application Patching

1

- Firewalls, VPNs, and Data Transfer appliances have shown to be vulnerable to numerous CVE exploits, including both unauthenticated access and Remote Code Execution exploits. Timely patching of these devices is critical to ensuring these devices are protected from the most recent exploits.
- Legacy Operating Systems are out of support and known vulnerabilities are no longer being patched. Current operating systems have patches for known vulnerabilities. Patching these vulnerabilities can assist in preventing unauthorized access or elevating privileges should unauthorized access occur.
- Remote Management Tools, VPN client applications, and office software suites have been found to contain exploits which can allow for remote access, unauthenticated access, and privilege escalation.
- Forward-facing Application servers, such as web-servers, ticket and project management servers, email servers and SQL servers have been shown to be vulnerable to numerous CVE exploits. It is important to keep these applications and any underlying frameworks they may utilize patched.

Email Filtering and Web Security

2

- Phishing emails, Search Engine Optimization (SEO) poisoning, and URL spoofing are three common techniques used by threat actors to gain a foothold in a corporate environment.
- Third party email applications can be utilized to help filter suspicious or malicious emails, email attachments, or email links before they even arrive in a user's inbox.
- Third party web filtering applications can be used to help prevent access to sites containing potentially harmful content or spoofed sites that are made to look like legitimate websites.

End-User Education and Phishing Training

3

- End-users pose the biggest threat to an internal environment and are also the organization's first line of defense. Users should be trained on how to identify suspicious attachments, suspicious emails, suspicious multi-factor authentication
  - attempts and how to do URL link verification. End-users should be trained on company policy with regards to acceptable browsing policy.
- Third party services such as KnowBe4 can be used to test the organization and identify areas needing improvement.
- Ensure users have clear guidance on communication channels and procedures should they encounter a suspicious email or have any questions.

Multi-Factor Authentication (MFA)

4

- Any forward-facing device or service with an externally accessible authentication page will become the target of attack. These attacks include brute-force password attacks, credential harvesting attacks, and CVE exploitation. The common mitigation steps recommended by most vendors are patching and to enable multi-factor authentication.
- MFA helps ensure the person authenticating is the actual end-user by means of a secondary authentication methodology which only the legitimate end-user should have access to.
- MFA should be implemented for external and internal network access as well as access to commonly used SaaS applications and email. This needs to include administrators and service accounts (especially third-party service accounts on a domain).

Endpoint Detection and Response

5

- Endpoint Detection & Response (EDR) toolsets provide behavioral-based detection capabilities in addition to typical signature-based analysis.
- This is a critical defense in preventing malicious actors from gaining access to an environment and running malicious tools which are either recognized as malicious or are currently unrecognized. Behavior analysis can also recognize activities known to be malicious such as dumping the LSASS memory service for passwords.
- Correct configuration of the EDR tool is critical to preventing attack. Ensure the EDR agent cannot be disabled or stopped without a password. Configure the console to stop suspected malicious activity first, possibly isolate the system and then alert to the activity for review.
- Insureds face a substantial challenge in internally managing and acting on any alerts generated by the EDR tool. 24x7 SOC monitoring by a third party is highly encouraged.

Password and End-User Account Management

6

- Over time any entity will have several employees come and go. Ensuring only active end-users maintain access to the corporate environment and email system is critical. Removing old accounts can prevent a legacy account from accidentally getting re-enabled. The same goes for old administrative and service accounts no longer being used.
- End-users are creatures of habit and like to use the same password or slight variations on old passwords to comply with password policy. Entities should create a strong password policy, ensuring passwords are changed regularly, have complex passwords, and do not match recently used passwords.
- Group membership is equally important to ensure employees only have access to the privileges and resources they need.

Event Logging

7

- Exporting logs to a System Information Event Management (SIEM) solution or syslog server is highly recommended. Memory based logs, such as those stored in firewalls are extremely limited and roll over quickly. Proper preservation of this information is key to a thorough forensic investigation.
- Ensure devices are logging useful information. Firewalls should be recording source/destination IPs and bytes sent/received for each session. Make sure both accepted and denied traffic are logged. Management review portals are good for spotting potential anomalies, but do not provide the granular details necessary to assist with a forensic investigation.
- Logs should be exported from items such as Firewalls, VPNs, EDR solutions, MFA solutions and critical server event logs.
- Consider enabling access auditing for sensitive data files which might contain PII/PHI/or confidential data.
- Disk storage capacity and retention period of the data should be considered.
- Consider using a cloud hosted SIEM such as Elastic or Splunk for offsite aggregation. Logs are of no use if the SIEM server is a virtual machine that becomes fully encrypted.

Backups

8

- Onsite backups allow for quick restoration of files but are typically identified and attacked by threat actors either through deletion or encryption, especially for backups on Network Attached Storage (NAS).
- Offsite backups provide some protection from threat actors. Offsite backups are typically slower as they require downloading the data from the cloud or transporting data from a storage facility back to the office to restore.
- If backups are stored offsite, check if the storage provider retains backups copies and if there are protections in-place to prevent deletion of the backups. Immutable backups are preferred as they cannot be deleted or changed. Ensure the backups cannot be deleted by email or telephone call without some type of additional verification. A verification password is not a good verification option if it is stored in the company network or email system.

Know Your Environment, Asset List, Software List, & RMM/RDP Tool

9

- Have a network diagram and asset list for all systems in the corporate network. Keep both up to date as network changes are made and as new devices are added or retired.
- Have a list of authorized software in the environment. Review the network regularly for unauthorized software and uninstall it. Remove software which is no longer used or needed. Particular attention should be paid to tools which threat actors can use to "live off the land". This includes RMM tools, data transfer tools and network reconnaissance tools.
- Only use approved Remote Monitoring and Management tools (RMM). Ensure the software requires multi-factor authentication, if available. Do not allow employees to install their own RMM tools. Require employees needing remote access to only use approved methods with the necessary safeguards in place.

Incident Response Planning and Testing

10

- Have a written plan in-place covering all aspects of IT staff responsibility in the event of an incident.
- Conduct testing and simulation of an incident with the personnel who would be involved in the response.
- Ensure IT personnel have 24x7 contact information for decision makers. Time is critical during an active incident. The decision makers will need to have the correct information quickly to assess initial steps such as whether to disconnect systems, isolate systems or completely disconnect the company from the internet.
- Preservation of evidence is key to a forensic investigation which may be needed to assess potential notification obligations. Make sure IT staff knows which tools are available for system preservation and are trained on them. Look at having additional storage on-hand if compromised virtual machines need to be offloaded, or disk images need to be created.
- It is best to have backups stored both onsite and offsite.

ABOUT THE AUTHORS

CAROLINE MCGLYNN

Caroline McGlynn, Esq. is an accomplished attorney and business professional with over two decades of experience spanning law, business development, and commercial strategy/operations. She currently leads the Global Business Development team for Booz Allen's Commercial Incident Response (IR) Business, where she and her team build and expand key alliances with insurance carriers, brokers, cybersecurity vendors, and law firms. Booz Allen's IR team handles more than 1,000 investigations a year for a range of clients, including many in the Global Fortune 2,000. Booz Allen's Commercial Business is centered around cybersecurity – planning/assessment, incident response, and transformation/resilience – and Caroline works with both the IR and Enterprise Consulting teams every day.

Caroline began her career as a prosecutor in Philadelphia, quickly becoming the youngest Bureau Chief in the organization's history. While at the District Attorney's Office, Caroline managed a large team of prosecutors and investigators while personally trying hundreds of cases, including homicides and other violent felonies. In addition to maintaining an active caseload, Caroline led numerous successful crime- reduction initiatives and developed new public policies, traveling nationally to assist other jurisdictions with similar pursuits.

Transitioning to the private sector, Caroline joined Fox Rothschild, LLP, where as a Partner she represented clients in complex commercial litigation and regulatory compliance matters. After Fox, Caroline joined SentinelOne, a leading AI-based software development company. At SentinelOne, Caroline was the Americas business development lead, managing external partnerships in the Incident Response and Cyber Risk ecosystem.

Contact Caroline McGlynn: mcglynn_caroline@bah.com

ABOUT THE AUTHORS

JENNIFER POLLIARD

Jennifer Polliard is a Director at Booz Allen and leads the Threat Actor Communication & Intelligence (TACI) team for the commercial Incident Response business. A 25-year veteran of local law enforcement and the military police, Jennifer is an experienced negotiator who has handled thousands of crisis negotiations during her career.

Jennifer has a proven track record in intelligence gathering, strategy development, and crisis communications/negotiations, which she uses as she leads a team of experts who navigate hundreds of ransomware events and other cyber incidents each year. Jennifer and her team work with a broad range of companies across every business sector, from small, privately owned organizations to the Global Fortune 2,000. Jennifer and her team successfully negotiate and communicate directly with adversaries by using data-driven intelligence and tracking the behaviors/patterns of threat actor groups (both independent and nation-state affiliated). The TACI team also works closely with clients to proactively develop strategies to mitigate ransomware incidents.

In addition to her round-the-clock work assisting clients, Jennifer is an oft-sought keynote speaker and presenter on ransomware negotiations. Jennifer also helps legal counsel prepare for litigation related to cyber incidents, including acting as an expert consultant and courtroom witness.

An advocate for women in cybersecurity, Jennifer serves as a mentor and often speaks to individuals and organizations that are focused on recruiting women into cybersecurity and advancing women in the field.

Contact Jennifer Polliard: polliard_jennifer@bah.com