ISSUE 143
BOARD PERSPECTIVES

RANSOMWARE: ANALYZING RISK AND PROTECTING CRITICAL ASSETS

Ransomware is a current threat many people are struggling to understand and manage. Amid the headlines and uncertainty, how can the board respond strategically?

The WannaCry and NotPetya attacks in 2017 got everyone's attention as to the potential devastation ransomware incidents can leave in their wake. Since then, these attacks have continued unabated against one organization after another until, in 2021, the high-profile Colonial Pipeline and Kaseya attacks once again proved that the perpetrators of these crimes play for keeps.

Reputation damage, hefty ransoms and business continuity are all concerns with ransomware. But the core of the conversation is about the potential loss of intellectual property and customer information and the specter of unpleasant dealings with criminals and other parties who may or may not be sponsored by nation-state actors.

The market still doesn't know the number and full scope of these attacks, as few companies victimized by them are eager to share their experiences. However, estimates of total ransomware costs in the United States run as high as $20 billion in 2021.[1] The average ransom demand has tripled.[2] As underwriting standards elevate the need for additional security controls, it may become more difficult for organizations to qualify for cyber insurance.

Several things are clear: Few companies are fully protected and no company feels safe from ransomware. And every company, regardless of size or location, is vulnerable.

Today's ransomware threat actors focus on disruption. They no longer remain silent for months inside a company's technology systems, awaiting the payoff of exfiltrating

1 "The 2021 Ransomware Statistics, Data, & Trends You Need to Know," by Raffi Jamgotchian, Triada Networks, May 30, 2021: https://triadanet.com/ransomware-statistics/.

2 "Ransomware Payment Demands Triple in 1H 2021, Coalition Reports," by D. Howard Kass, MSSP Alert, July 30, 2021: www.msspalert.com/cybersecurity-research/ransomware-demands-triple-coalition-reports/.

protiviti®
Face the Future with Confidence

data. Emphasizing velocity, their model is to rapidly penetrate, exfiltrate, encrypt and then demand ransom, all within a matter of minutes.

Ransomware was once automated malware that haphazardly encrypted data. Now, it's much more. The current generation of ransomware campaigns initially uses live-off-the-land techniques combined with specialty tools that are highly obfuscated to avoid detection. Dwell times average four to six weeks, as attackers curate data exfiltration for maximum impact. Victims refusing to pay extortion must prepare for public disclosures of exfiltrated data. The bottom line is that rogue players end up controlling the enterprise.

The economics of ransomware are evolving, too. Ransomware as a service (RaaS), an offering of pay-for-use malware, can be invoked to encrypt systems and collect the ransom, shortening cycles between campaigns. Similarly, attackers running campaigns can buy access to networks through an open marketplace.

Boutique services have evolved among security providers to negotiate and pay the ransom on behalf of clients. In the U.S., several state legislatures are considering banning ransomware payments, while the FBI is advising the U.S. Congress against such bans.[3] Navigating these trends often requires expertise with a deep understanding of the business.

As attacks, and the attackers themselves, become increasingly sophisticated and the consequences continue to magnify, companies must learn and respond in kind. To adapt confidently to this evolving threat landscape, they must combine operational resilience, cyber threat intelligence and cybersecurity.

But this isn't easy. There are many moving parts to consider when building a robust, coherent and dynamic cyber defense system that responds to the attack landscape with focus and speed. Examples of these moving parts are illustrated below:

WHERE WE WERE COMPROMISED	HOW WE COULD HAVE STOPPED IT	
User reuses credentials on websites	• Security awareness training	• Culture of compliance
Attacker finds credentials or access for sale	• Cyber threat intelligence • Password policy controls	• Vulnerability management
Attacker accesses vulnerable systems	• Multifactor authentication (MFA) • Geofencing	• Advanced threat protection
Attacker acquires privileged identity	• Advanced threat protection • Privileged identity/access management	• Strong access management
Attacker curates collection of data to steal	• Data loss prevention • Intrusion detection systems	• Endpoint detection and response
Attacker triggers ransomware	• Endpoint detection and response • Backup hygiene	• Cyber insurance
Attacker follows with an extortion demand	• Incident response • Law enforcement	• Crisis management

Given the complexity and dynamics of ransomware exposures, what can board members do to help their organizations meet the challenge of analyzing risk and protecting critical assets? We offer four suggestions on the following pages.

[3] "Top FBI official advises Congress against banning ransomware payments," by Maggie Miller, *The Hill*, July 27, 2021: https://thehill.com/policy/cybersecurity/565110-top-fbi-official-advises-congress-against-banning-ransomware-payments.

PREPARE THE CHIEF INFORMATION SECURITY OFFICER (CISO) FOR SUCCESS

Some CISOs find the prospect of addressing the board intimidating and may not feel they're up to the task. Others may perceive they can't get traction on budget requests and aren't in a position to self-advocate.

Most CISOs recognize that they must speak in a manner that resonates with the board and frames the conversation at the appropriate level. But they may lack the strategic communication skills that are so important in the boardroom.

As the CISO's role is so essential to the hygiene and security of some of the enterprise's most important assets, it's a two-way street for both the board and the CISO to maximize the value of their interactions. The board should:

- Instill confidence in the CISO by clarifying expectations, educating itself on the issues, allowing sufficient agenda time for discussion, and paying attention when additional resources and budget are requested.
- Assist the CISO in focusing preparations, priorities and metrics for the boardroom by conveying its concerns.
- Under the auspices of the board or committee chair, let the CISO deliver the message in response to the stated expectations and take questions requiring a more detailed response offline if limited agenda time is allotted to the cyber discussion.
- Position the CISO as a strategic partner at the board level, with necessary interfaces between meetings with interested directors and active support from the board chair and CEO.
- Consider the CISO an education officer who will help the board understand the gravity of the issues.
- Understand and approve management's criteria for recruiting and hiring the CISO and succession planning for the position.
- Ensure that candidates for this role have a strategic view, understand the language of the boardroom and aren't just mired in operational response; that will help them delineate content that has value.

ORGANIZE THE BOARD FOR EFFECTIVE CYBERSECURITY OVERSIGHT

When a ransomware attack occurs, the full board often owns the matter and is engaged until the issue is resolved and the system's structural integrity is restored.

The maintenance of that integrity going forward is the primary focus of either the full board or a designated board committee.

The CISO owns the plumbing underlying the operational response and management is responsible for its effectiveness. However, directors should expect to gain confidence from the CISO's briefings about the response plan going forward and any third-party vendors engaged to assist in its implementation. Everyone involved should reflect on the lessons learned from past attacks and continuing assessments of the threat landscape.

The board should periodically assess whether it needs access to additional expertise — either as a member of, or an objective adviser to, the board.

Relevant options for structuring board inquiries depend on the severity of the threat landscape, the role of technology in executing the company's business strategy, and the sensitivity of the systems and data supporting the business model.

ASK THE RIGHT QUESTIONS — AND DON'T OVERLOOK THIRD PARTIES WHEN ASKING THE RIGHT QUESTIONS

Many boards seek to understand how ransomware attacks have occurred elsewhere and whether cybercriminals could exploit those same methods in their own organizations.

Directors should not underestimate the importance of asking the right questions of management on situational awareness, strategy and operations, insider threats, incident response, and related topics. An appendix in a National Association of Corporate Directors (NACD) publication on cyber risk oversight suggests relevant questions.[4]

For ransomware, directors should focus on compromise assessment and on incident response and preparedness, with an end-to-end view of the enterprise:

- A ransomware attack on third parties handling mission-critical systems and sensitive data can stop the show, just as a direct attack on the company can.
- If attackers discover a third party's access privileges to company systems and data, then the company itself could come under attack.

Continued ...

[4] See Tool A: *Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards*, NACD, 2020, available for purchase at www.nacdonline.org/insights/publications.cfm?ItemNumber=67298.

SUPPORT THE CONVERSATION WITH A DASHBOARD OF APPROPRIATE METRICS	
The CISO's reporting and metrics should inform board communications and be integrated into the overall enterprise risk management (ERM) dashboard.	Relevant metrics might include: • The number of system vulnerabilities • The length of time required to implement patches • The number of breaches • Attacker dwell time (the length of time it takes to detect a breach) • The length of time it takes to respond to a breach, once known • The length of time it takes to remediate audit findings • Percentage of breaches perpetrated through third parties • Number of violations of security protocols Attacker dwell time is particularly critical to a ransomware attack. The longer attackers remain undetected in a network, the more likely they will be able to find systems and resources they can leverage for ransom.

Today's ransomware attackers often are well-funded, possess business savvy and are highly skilled in hacking methods. And they're playing tough. While the board isn't responsible for day-to-day operational details, its duty-of-care responsibilities in the cyber space are significant given the sensitivity of data and the value to shareholders of the company's intellectual property, reputation and brand image.

Questions for Boards

Following are some suggested questions that boards of directors may want to consider, based on the risks inherent in the company's operations:

- Do we have effective security controls designed to prevent or limit the impact of ransomware?
  - Are cyber controls in place to protect our privileged-access accounts?
  - How often are these controls tested? Are tabletop exercises of likely attack activity — given the increasing sophistication of threat actors — performed periodically to ensure defenses can detect a breach and respond in a timely manner?
  - What is our backup strategy to mitigate ransomware? For example, do we have a consistent backup cadence and are backups stored in off-site locations?
  - Should we experience a ransomware attack, what is our incident response plan? How broadly is the plan shared within our organization? Do we have a provider on retainer in the event we are the target of a ransomware attack?
- Do we know where our critical systems and data reside, the critical assets that we simply cannot afford to lose or have taken away, and/or systems for which unplanned shutdowns can't be tolerated? Do we have the processes in place for operational resilience? Do we have 24x7 defense and monitoring against a ransomware event?
- Does the company have cyber insurance with provisions for extortion coverage, including investigatory costs, negotiations costs, ransom payments and other incidental losses?

Continued ...

- Does the board define its expectations for the CISO and management in the cyber space and establish clear accountabilities for performance?
  - If the organization has a risk appetite statement, are the board's expectations for cybersecurity and ransomware attacks incorporated therein?
  - Do the metrics used by management and reported to the board provide supporting key performance and risk indicators as to how the top-priority cyber risks are being managed? Do they address areas that inform the board's oversight and the CISO's communications with the board?
  - Can we effectively quantify the impact of a ransomware event?
- Does the transition to remote or hybrid work arrangements and reliance on virtual business-to-consumer (B2C) experiences, as spurred by the pandemic, increase the risk of targeted criminal ransomware attacks and advanced persistent threats? Are we addressing the risk of criminals exploiting remote workers? Does our third-party risk management program consider potential exposure to ransomware attacks?

How Protiviti Can Help

Protiviti's newly expanded and specialized Ransomware Advisory and Recovery offering within our cybersecurity and privacy practice helps companies manage rising threats from malicious actors attacking and disrupting mission-critical operations. Our offering is designed to help organizations manage the short-term crisis of a devastating ransomware attack, get back to business and build toward long-term resilience.

Our cross-solution teams help clients strengthen their ransomware resilience and broader cybersecurity posture across their business via three key phases — anticipate, respond and recover. With operational resiliency a high priority for boards and C-suite executives, strong crisis management plans and up-to-date data protection are critical to sustaining daily operations, improving efficiency and recovery time, and becoming a more secure organization.

CONTACTS

Terry Jost
Global Security & Privacy Segment Leader
+1.469.965.6574
terry.jost@protiviti.com

David Taylor
Managing Director
+1.407.849.3916
david.taylor@protiviti.com

protiviti®