the BULLETIN

Protiviti's Review of Corporate Governance

Volume 7, Issue 11

Ransomware: Preventing an Attack and Responding to and Recovering From an Attack

Ransomware attacks have been around for many years. In the past, cyber-threat actors would penetrate a company's computer and network systems and obtain data with the objective of returning it upon payment. The demanded payments were usually smaller than the ransoms requested in recent incidents. Also, companies could either work their way out of the situation using their data backups to restore IT systems and business operations or negotiate a lesser payment. Most of these incidents weren't financially material, nor were they reported publicly.

By contrast, today's ransomware perpetrators execute well-orchestrated attacks typically accompanied by more significant financial demands. These incidents don't focus on simple "theft" of data; instead, their intent is to disrupt the business. Several recent, well-publicised incidents totally locked down organisations by exfiltrating all data and/or all access to business networks, applications and data, effectively halting critical business processes.

During a ransomware event, cyber attackers may contact and converse directly with their victims, offering a well-articulated list of demands along with clear threats of further business disruption if demands aren't met. The attackers may bargain over the amount of payment, promoting quick resolution to the attack, with guarantees of full recovery when their demands are satisfied.

The impacts to businesses affected by a ransomware attack can take many forms, depending on the company's operations, financial strength and arrangements with third parties to assist with a ransomware work-out. Several recent attacks have targeted businesses in industries — for example, consumer products and other business-to-consumer (B2C)-related industries — where the level of cybersecurity investments is generally less than businesses with higher security profiles, such as those operating critical infrastructure or subjected to regulations prompting increased investment in cybersecurity.

Preventing a Ransomware Attack

Companies affected by ransomware become victims when a perpetrator finds a security weakness that enables access to an organisation's systems. Aggressive ransomware gangs use various techniques to gain access to systems. Common strategies include:

- Using stolen credentials to access systems where ransomware can be installed. Attackers might obtain credentials through phishing campaigns or other social engineering tactics or purchased from dark web sources.
- Tricking a user into installing ransomware onto their device. An example of this attack vector is emailing a link or attachment that the user opens and installs.
- Exploiting failure to remediate or "patch" a known cybersecurity vulnerability. For example, Microsoft Exchange servers recently had a vulnerability patched. Microsoft urged exchange customers to apply patches immediately. Unfortunately, some organisations fail to apply patches in a timely manner, leaving themselves with known vulnerabilities that adversaries can easily penetrate and exploit.

The following table focuses on countermeasures businesses can use to address these issues:

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

As noted above, the human perimeter may be just as important as the technical perimeter. Simply stated, the cybersecurity mindset of a company's employees may be one of its most important ransomware defence mechanisms. Their awareness of the risks and vigilance as data defenders make it more difficult for cybercriminals to obtain sensitive information or deceive unsuspecting users into downloading an infected file. Training and constant reinforcement through simulated phishing email testing can transform employees into a resilient line of defence against unusual email messages, attachments from unfamiliar parties and running unrecognised apps downloaded from the internet.

Anti-malware software, kept up to date, offers protections from phishing and malware attacks by detecting and blocking malicious files and warning users when they're visiting suspicious websites. Secure email gateways filter inbound and outbound email communications to identify threats and prevent their delivery, stopping ransomware files in their tracks. Post-delivery protection solutions powered by machine learning systems or artificial intelligence algorithms can stop advanced email threats that penetrate the email network. Organisations can also use web-filtering solutions to restrict user access to certain websites.

Responding to an Attack

The impact of ransomware attacks has increased in velocity. Early ransomware consisted of automated malware that haphazardly encrypted data. Now, it's much more. The current generation of ransomware attacks are orchestrated through preplanned, strategic campaigns of reconnaissance, penetrating the organisation's attack surface, and quickly exfiltrating data. Campaigns continue with the extortion receipt, outlining actions requested of the victim.

If a business finds itself under attack, it's critically important to follow all established cyber-incident response plans and operational resilience protocols to manage the incident. Due to the holistic impact associated with modern-day ransomware attacks, managing the actual incident requires a *larger-scale crisis management approach*. Such an approach enables organisations to effectively address the broader list of business processes these attacks impact, including the initiation of full recovery and data verification post-attack.

An in-process ransomware situation requires many new procedures, processes and skills to combat the attack. Examples include:

- Interacting with cyber insurance companies. These firms are often immediately engaged when an attack occurs if the policy includes extortion coverage and covers the costs to investigate a ransomware attack, negotiate with the perpetrators and make a ransom payment. Note that as the frequency and severity of attacks escalate, cyber insurers can be expected to encourage their policyholders to implement cybersecurity best practices proactively to minimise the likelihood of having to pay out ransomware claims.
- Many companies seek outside legal counsel who have ransomware experience to help negotiate ransomware payments. Many important questions can be determined in advance; however, executive decisions will be made during the crisis, including the process to determine payment if a company reaches a negotiated agreement to proceed with a payoff.

> *The cybersecurity mindset of a company's employees may be one of its most important ransomware defence mechanisms.*

- Crisis and related decision-making can be chaotic if an attack impacts essential business functions. Robust contingency plans should cover day-to-day business operations for essential supply chain, financial and human resources requirements, which may revert to 100%

manual effort to manage the business through the duration of the crisis.

- Most ransomware attackers insist that their targets pay ransoms in digital currencies, such as bitcoin. Companies may want to proactively contact a bitcoin exchange and discuss the process and time required to open an account and inquire about escrow facilities to manage payments safely.
- The decision as to whether or when a company engages law enforcement is a policy matter. Such engagement often depends on the magnitude of the ransom payment and whether there are opportunities to litigate (although the probability of recovering damages through litigation is typically low). As some of the most recent ransomware events have resulted in larger payments and required direct negotiations with attackers, best practices for containing ransomware attacks continue to evolve. In the United States, the Biden administration is pushing for mandatory disclosure to the federal government about ransomware attacks, cyber incidents that affect critical infrastructure, and other breaches creating risks to the government and the public. If adopted, this measure would reinforce the Federal Bureau of Investigation's long-standing encouragement that ransomware attack victims notify law enforcement.[1]

The following table provides a summary of countermeasures when responding to an attack:

WHERE WE WERE COMPROMISED	HOW WE COULD HAVE STOPPED IT	
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

Obviously, an important consideration is whether to pay the ransom. If the company has backed up the encrypted systems and data, management is in a much stronger position to negotiate. Otherwise, the business must assess the value of the encrypted data loss against the requested ransom. Another important consideration: Paying the ransom doesn't guarantee that the cybercriminals will return access to the stolen data. Furthermore, the malware remains in the system, requiring a thorough cleansing of the system after the attack.

Recovering From an Attack

In the aftermath of a ransomware attack, it's first things first: Conduct a postmortem on why and how it happened and take corrective action to prevent and detect future attacks more effectively. This assessment entails understanding how the attacker obtained the access needed to enable encryption and lock down company data. To that end, endpoint detection and response solutions — which continuously

[1] "Biden Administration Wants to Require Businesses to Disclose Ransomware Attacks," Masood Farivar, VOA, July 27, 2021, available at www.voanews.com/silicon-valley-technology/biden-administration-wants-require-businesses-disclose-ransomware-attacks.

monitor all incoming and outgoing traffic on a network for potential threats — can provide transparency as to where the attack started and how it progressed. The business can use this insight to help prevent similar incidents from happening again.

Erasing ransomware from company systems is a priority in the aftermath of an attack. This task can be very difficult to accomplish with confidence if the criminals don't provide the keys to decrypt the infected files. And, even if they do, how can management be confident the files are fully cleansed without wiping down all files and storage devices and starting anew?

Using prior data backups can reduce the severity of an attack's impact on the business. Daily data backups should include processes to store data off-site, without any connections to the organisation's IT systems. When possible, backup processes should use routines with point-in-time recovery, meaning data is recovered as close as possible to the precise time of the attack. This capability facilitates a more rapid recovery. That said, it's surprising how many companies don't have a consistent backup cadence or fail to store backups in off-site locations. Accordingly, business IT executives should consider continuous backup process monitors and verification.

Resilience Is the Name of the Game

Prevention, response and recovery are all about operational resilience, or the organisation's ability to detect, prevent, respond to, and recover and learn from cyberattacks and other operational disruptions that may impact delivery of important business and economic functions or underlying business services. The key components of resilience — which include defining and understanding important business services and impact tolerance, as well as completing end-to-end mapping, scenario testing and regular self-assessments — are essential guideposts to managing the risk of ransomware attacks. There are six components to achieving resiliency:

- **Evolve governance and culture**. Establish proper governance functions and implement a resilience programme based on the needs of the organisation's important business services. For example, develop real-time operational resilience dashboards, reporting and cultural levers that will evolve enterprise behaviour.
- **Identify important business services and processes**. Understand the critical business services and processes given the company's regulatory obligations or established criteria that focus on the importance to customers and other stakeholders.

> *If the company has backed up the encrypted systems and data, management is in a much stronger position to negotiate.*

- **Establish front-to-back mapping of important business services and processes**. Build on existing continuity practices to establish and maintain comprehensive mapping of critical processes, applications, third parties, and other components that contribute to the delivery and execution of important business services and processes.
- **Define "intolerable harm" and establish impact tolerances**. Understand the impact of an operational resilience event on the various stakeholders of the company and identify the most critical areas affected. Establish impact tolerances for

important business services. Extending beyond traditional recovery time, impact tolerance represents the point at which an interruption threatens intolerable harm to applicable stakeholder groups.

- **Scenario test and improve**. Test "extreme but plausible" scenarios to understand better the realistic recovery times versus established impact tolerances. Testing will indicate where the business should invest in technology or processes to stay within established tolerances. Lessons learned through testing should be considered and acted on to continue to improve resilience.
- **Self-assess**. Identify key resiliency risks (e.g., by theme, function, domain) and design detailed, deep-dive assessments that drive outcomes in line with industry standards and regulatory expectations. Create measurement mechanisms that can demonstrate change and resiliency improvement.

Resilience is a market expectation of mature organisations — and it extends to a ransomware attack. Having a solid understanding of how to minimise the impact of a ransomware disruption to external stakeholders and the broader economy, knowing where the organisation's vulnerabilities lie, and developing cyber resilience will help the business respond and recover more quickly from an attack and minimise customer harm.

Resilience is a market expectation of mature organisations — and it extends to a ransomware attack.

Final Thoughts: Questions to Ask

The costs of ransomware attacks are rising. The business impacts of system downtime, people time, public embarrassment and potential reputation loss can make the financial value of the ransom payment pale in comparison. As ransomware campaigns continue and target more companies, it's time for executives to ask tough questions, such as:

- Do we have effective security controls in place that are designed to prevent or limit the impact of ransomware? How often are these controls tested?
- Do we know where our critical data resides? Do we have the processes and components in place for operational resilience?
- Can we effectively quantify the impact of a ransomware event?
- Do we have 24x7 defence and monitoring against a ransomware event?
- Are cyber controls in place to protect our privileged-access accounts?
- What is our backup strategy to mitigate ransomware? Do we have a consistent backup cadence and are our backups stored in off-site locations?
- What is our incident response plan if we're the target of a ransomware attack? How broadly is the plan shared within our organisation?
- What are our incident response capabilities? Do we have a provider on retainer?

How Protiviti Can Help

Protiviti is helping CISOs, CIOs, CAEs and CDOs navigate the rapidly evolving cybersecurity landscape. Our enhanced ransomware offering within our cybersecurity and privacy practice helps companies manage the rising threat levels to their business from malicious actors attacking and disrupting mission-critical operations. The newly expanded and specialised Ransomware Advisory and Recovery offering is designed to help organisations manage the short-term crisis of a devastating ransomware attack, get back to business and build toward long-term resilience.

Our cross-solution teams are helping clients strengthen their ransomware resilience and broader cybersecurity posture across their business via three key phases:

1. **Anticipate:** Forecast, understand and counter threats with an active defence.
2. **Respond:** Manage the crisis once a ransomware attack is underway, engaging executive, legal and technical stakeholders while managing business requirements.
3. **Recover:** Post-attack, ensure operations are restored, reinforce security systems and rebuild organisational resilience.

As operational resiliency continues to be 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 organisation.

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