METROPOLITAN
CORPORATE
COUNSEL®

OCTOBER 2017 WWW.METROCORPCOUNSEL.COM

SPECIAL SECTION: CYBERSECURITY

Ready for Ransomware

Companies may not be able to prevent malware attacks, but they can prepare for them

Ransomware is much in the headlines of late, with the widespread and high-profile Petya attack just months ago. ***Gretchen Ruck****, a director at* ***AlixPartners LLP*** *in New York, explains why ransomware isn't as straightforward as it sounds and how the best tactic for defense is to pull cybersecurity discussions into the C-suite light of day. The interview has been edited for style and length.*

Please describe a ransomware attack, the motives behind it, and what it looks like to the victims. How is a ransomware attack different from other breaches?

Gretchen Ruck: At its core, ransomware is a form of malware intended to prevent victims from accessing their data. When most people think of ransomware, they envision a chaotic scenario in which a cybercriminal haphazardly unleashes an attack that harnesses software vulnerabilities, allowing the attacker to encrypt the unsuspecting victim's system and then demand money in exchange for code necessary to unlock it. It's true that ransomware attacks frequently follow this pattern, but the methods of these attacks and motives behind them have become more varied.

In addition to asking how companies should respond and who should be notified, we should also be asking who will be held accountable.

While other types of cyberattacks focus on stealing and exposing confidential data or committing theft through deception or collusion, ransomware focuses on hindrance through loss of availability or denial of access to systems or files. The attacker usually achieves this by encrypting the victims' data or taking over their accounts and resetting their passwords.

Most often, these attacks are delivered via a phishing email attachment or a malicious website link that surreptitiously downloads malware aimed to exploit an unpatched security flaw or a software vulnerability. Recently, as demonstrated by the Petya ransomware attack at the end of June, instead of initiating the attacks by email, they may be propagated through seemingly routine third-party software updates that deliver a payload of embedded malware.

Though the name ransomware suggests the motive is money in exchange for returning control of data or resources, attacks have become more nefarious lately and some can be characterized as wiper attacks, which destroy data with no hope of restoring it. The Petya attack was intended to be destructive in nature – the data wasn't released in exchange for the demanded ransom. Instead, the attack provided a way to shut down businesses, perhaps because of radical opinions, to impact market share and competition, or to influence situations for political advantage.

For the most part, ransomware hasn't typically been a targeted attack focused on high-value data, but that could be evolving. Targeted threats have traditionally been linked to mining for confidential data with the intent to steal it, and to integrity incidents. As the cybercriminals who execute these

Gretchen Ruck, *a director at AlixPartners LLP in New York, has 20 years of experience in lead security and risk roles and, as a trusted advisor, in consulting roles at global organizations and government agencies. Ruck helps businesses quickly identify what's really at risk by pinpointing critical, executable improvements focused on protecting high-value data and securing key assets from threats and malicious actors. She can be reached at gruck@alixpartners.com.*

attacks become savvier, combining the wiper intention with longer-term persistence could signal the beginning of denial and disruption campaigns against U.S. companies.

What can companies do to defend against ransomware attacks, and how have those practices changed over the past few years?

Ruck: Just within the last year or so, ransomware has really taken center stage as a business risk. It's likely going to continue its reign as one of the top cybercrime risks over the next year or so. Cybercrime morphs very quickly. With each new attack, we see modified approaches and new exploits incorporated. The advice I provide concerning ransomware attacks applies more broadly to any malware attack.

To defend against an attack, you need to start with the basics. This includes good security hygiene, such as employing mature security administration, maintenance, operations, monitoring, event management, vulnerability and patch management processes. It also helps to align these processes with recognized industry guidance, such as ISO27000, NIST or SANS20, to ensure a comprehensive set of security controls are in place.

As the next step, companies need to identify and prioritize safeguarding high-value data and business-critical systems. Inventorying and classifying systems based on business criticality and data sensitivity establishes the appropriate levels of security control to incorporate and test against. This should include resiliency, redundancy and recovery requirements for all technology developed in-house and acquired through procurement. Your most valuable data and critical business systems should not only be backed up periodically, but there should also be another site where they are actively mirrored in real-time to allow for failover capability.

Everyone plays a role in defending the company against security threats. Build a user base and customer base that are risk-aware. They should not just be trained on security responsibilities, they should also be engaged in the mission and vigilant in spotting new threats. Think of your security team as playing a role similar to that of a soccer goalie. In this analogy, your security team is not your only line of defense, but rather, they are your last line of defense. If a team expects their goalie to stop every single shot attempt, they're going to have a very worn-out goalie, and they're probably going to have a lot of goals scored against them. There are multiple lines of defense, and everyone has to play an active role. The same reasoning applies to stopping a typical cybercrime attack.

When evaluating security, it's surprising how frequently people treat business as something that's static. Businesses are constantly innovating and, to be effective, security must keep pace. Companies are striving to find ways to better leverage their data: to have more agility in how they engage with customers, to create more digitally augmented products, and to increase the use of automation and insight-driven decision-making within their companies. As they do this, they change their attack surface and impact their risk portfolio.

How should companies respond to a ransomware attack? Who needs to be notified in terms of law enforcement, employees, investors or the public in general?

Ruck: In response to an attack, timely reporting to stakeholders and to the user community is vital to avoid any lasting damage. Whether responding to a ransomware attack or any other security incident, successful responses follow scenario-driven playbooks that should be planned for and tested in advance. These plans should elicit involvement and partnerships between security, IT, general counsel, the business and, when necessary, law enforcement.

The plans should put processes into place to enable consistent decision-making regarding when to notify external stakeholders such as investors, customers and the public. As part of these plans, a pivotal and obvious question that organizations must be prepared to answer is how to handle incidents involving ransomware extortion demands. This should be discussed with leadership in advance of such an event occurring.

In addition to asking how companies should respond and who should be notified, we should also be asking who will be held accountable. Years ago, it may have been someone in IT; but, as cybercrime visibility and damages have increased, accountability has shifted upward. Around 10 years ago, we started seeing security regulations incorporate risk management into governance responsibilities in recognition of the need to align security to business operations.

Now, we're beginning to experience another shift. Top executives and boards must demonstrate their understanding of the organization's cybercrime risks when asserting business goals and in fulfilling their leadership and oversight responsibilities. If your organization hasn't shifted crucial security decision-making from the backroom to the boardroom, this should become an immediate priority. Due to the potential impact that a poorly handled security event could have on a business, boards need to be aware of the key security risks faced by the organizations they advise.

How can companies deal with reputation management if they find themselves the victims of a ransomware attack?

Ruck: Whether it's a ransomware attack or a breach of confidential data, follow your defined procedures and respond in a timely and transparent fashion. The organization needs to communicate a clear and consistent message. Within the incident response plan, include a communications strategy that engages your general counsel and PR team in incident remediation.

Be prepared to show that your organization has taken reasonable precautions and has a comprehensive set of security controls in place. These controls, which should map to identified risks, are expected to be verified periodically, to confirm that they consistently function as designed. Where you've identified security weaknesses, vulnerabilities and noncompliance areas, prioritize them based on urgency and begin making progress toward an improvement plan.

There is talk about companies sharing information about attacks to crowdsource their knowledge on how to prevent future incidents. For example, law firms by and large use the same systems. They buy software from the same companies. At the same time, there is concern about competition. Should they be collaborating about their experiences if they've been breached, are concerned about breaches or have identified attempts at breaches, to prevent future incidents?

Ruck: A very affirmative yes. There are a number of industry roundtables where chief information security officers get together and talk about common threats that they're facing and what they're seeing in terms of attacks. People who participate are responsible for keeping the discussions confidential and understanding what they can and can't share. Asking for general feedback on whether organizations are adopting new security techniques, such as if they are doing more around application isolation or webcasting – there's a lot of success in that, and in no way does it make a company more vulnerable. When used correctly, these forums can be very useful tools, especially in industries that traditionally have not invested as much in security, such as professional service firms, including law firms.