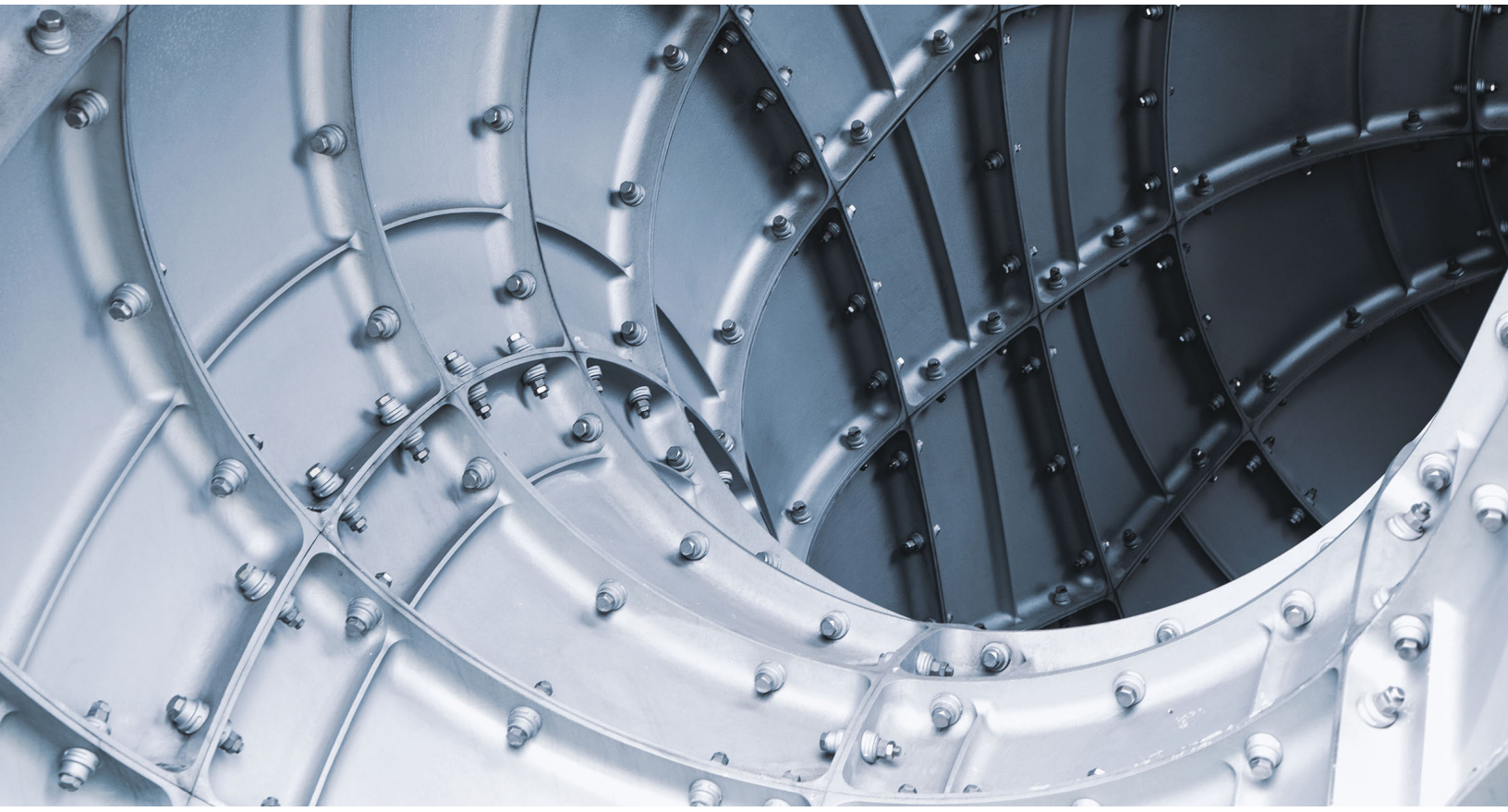
McKinsey & Company

Risk & Resilience Practice

Ransomware prevention: How organizations can fight back

Ransomware has rapidly become one of the top cybersecurity nightmares. Strategies for prevention, preparation, response, and recovery can help.

by Jim Boehm, Franz Hall, Rich Isenberg, and Marissa Michel



February 2022

No one can deny ransomware has hit new levels of sophistication, with demands for payment skyrocketing into the tens of millions of dollars. The reasons are manifold. Some are straightforward: vulnerabilities posed by pandemic-weary organizations and workers logging in from unsecured home networks; others are highly complex, such as ever-increasing connectivity driven by advancing digitization. Still other reasons include threat actors who are committed to perfecting their craft—rather than the "smash and grab" approach, hackers are now "dwelling" undetected within victims' environments to better understand where the highest value data and information are, and then selling that to other bidders. Finally, as the number of companies that are forced to pay ransoms to regain control of their networks and data increases, so does the number of hackers attracted to this type of lucrative threat.

To that end, Cybersecurity Ventures estimates ransomware costs should reach $265 billion by 2031.[1] Supply-chain attacks rose by 42 percent in the first quarter of 2021 in the United States, affecting up to seven million people,[2] while security threats against industrial control systems (ICS) and operational technology (OT) more than tripled in 2020.[3]

Sometimes looking at the overall numbers, it is hard to grasp the reality of a ransomware attack's effect on a company. To put it in perspective, here are some specific costs: Colonial Pipeline paid a $4.4 million ransom after the company shut down operations, global meat producer JBS paid $11.0 million, and global insurance provider CNA Financial paid a reported $40.0 million. Additionally, a ransomware attack on US software provider Kaseya targeted the firm's remote-computer-management tool and endangered up to 2,000 companies globally. These figures do not reflect the additional costs of an attack, including paying third parties, such as legal, PR, and negotiation firms, or the opportunity costs of having executives and specialized teams turn away from their day-to-day roles for weeks or months to deal with an attack and its aftermath, or the lost revenue that results.

With the use of low-cost ransomware-as-a-service (RaaS) campaigns, this cyberthreat has surged beyond the quiet confines of the C-suite to where boards of directors, regulators, law enforcement, industry associations, insurance providers, and the cybersecurity vendor community all need to be a part of the solution.

While governments, law enforcement, and regulators continue to grapple with ransomware issues such as transparency and oversight of cryptocurrencies, companies need to ensure they remain resilient by focusing on ransomware *prevention*, *preparation*, *response*, and *recovery* strategies. The payment or nonpayment of a ransom could well depend on whether an organization masters the basics of these four strategies and then continues to build higher levels of cyber maturity that create a resilient environment where attacks may still occur but do not have the same impact they would otherwise.

Prevention

To achieve a secure work environment, you need to know what technology you have, what and who it is talking to, and then watch it like a hawk. Vigilance is key. To get there, everyone from the board and C-suite to down the line must be on the same page and treat security as a continuous endeavor that balances technology with people and processes to ingrain security into an organization's DNA.

To achieve that balance, organizations need to understand that 75 percent of ransomware breaches begin with either a phishing email or a Remote Desktop Protocol (RDP) compromise, according to Coveware's quarterly ransomware reports for the fourth quarter of 2020 and the first quarter of 2021. In addition, it appears that in

[1] Daviid Braue, "Global ransomware damage costs predicted to exceed $265 billion by 2031," *Cybercrime Magazine*, June 3, 2021.
[2] Charlie Hart, "'Troubling' rise in supply chain cyber attacks," Supply Management, April 13, 2021.
[3] *ICS cybersecurity year in review 2020*, Dragos, 2021.

To achieve a secure work environment, you need to know what technology you have, what and who it is talking to, and then watch it like a hawk.

60 percent of ransomware cases, the malware ends up installed directly or via desktop-sharing apps, according to Verizon's 2021 *Data Breach Investigations Report (DBIR)*.[4] That just goes to show how crucial cybersecurity hygiene is across an entire organization, from employees and vendors to third-party supply chains. It is the first line of defense in mitigating a cyberattack. Companies are finding success with the following tactics:

— *Securing all RDP.* COVID-19 saw workforces shift to work from home—and home networks are often rife with poor security. Solid basic hygiene would include strong passwords, multifactor authentication, software updates, restricted access, and network-level authentication.

— *Multifactor authentication (MFA).* MFA for critical assets and high-risk users is strongly recommended. This tactic can be a strong barrier for attacks that leverage credential-based access or privilege escalation like ransomware.

— *Patch management.* Legacy systems, be it OT or IT, chug along on old software with security gaps. After RDP and phishing attacks, vulnerable software is the next largest attack vector, which is why securing communication channels and patching Windows operating system exploits remain vital.

— *Disabling user-level command-line capabilities and blocking Transmission Control Protocol (TCP) port 445.* Ransomware threat actors run free or low-cost software and scanning tools, searching for things like credential harvesting and internal unsecured port discovery from command-line prompts. If command-line capabilities end up disabled, the company becomes a more difficult target. Additionally, blocking port TCP 445 on external-facing infrastructure and internal firewalls also helps reduce the attack surface.

— *Protect Active Directory.* Active Directory is a database and set of services that connects users with the network resources they need to get their work done. The database (or directory) contains critical information about your environment, including what users and computers there are and who's allowed to do what.

— *Education and training.* Cyber awareness training and education should be mandatory. You don't need to be a highly trained and skilled cybersecurity professional, but basic changes in

[4] *2021 Data breach investigations report (DBIR)*, Verizon, January 2022.

behavior and awareness of where and how threats can enter your organization can further reduce risks.

Preparation

A core team—which includes senior leaders—that has worked to prepare for an attack is in far better shape to respond than one figuring it out on the fly. "The threat has really evolved from targeting big business to also targeting small and medium-size businesses," says Greg Hughes, CEO of Veritas, in a recent McKinsey article about recovering from ransomware. So, creating a business continuity plan and then practicing all types of scenarios will pay off. That includes the following:

— *Knowing your decision rights.* The timing, urgency, and stress of an attack escalate when decision rights are unclear. Who will lead the response team? Is the CEO directly involved or deliberately removed from the tactical details of response? After the business uncovers an attack, is the IT team fully empowered to take quick steps to stem the bleeding, regardless of business impact? And who will ultimately make the decision to pay and defend that decision internally and externally? Designate a person accountable for keeping the crisis response moving forward in a methodical and detailed manner and ensure decision trees end up aligned, from the chief information security officer (CISO) or chief security officer (CSO) to the CEO or response leader.

— *Preparing for all options and understanding negotiating constraints.* Prior to experiencing a ransomware attack, the majority of companies say they will not pay a ransom. However, when nearly two out of three organizations ended up victimized by a ransomware attack over the past 12 months, over 80 percent paid the ransom demands, according to a 2021 report from ThycoticCentrify on the state of ransomware. Constraints can range from the level of insurance coverage to whether customers' data are also at risk and premerger or preacquisition sensitivities. Given these will change over time, ensure this view is refreshed periodically.

— *Getting your board up to speed.* Generally, board members will want to help and bring issues to closure—the success of which all comes down to communication. That is why the board and executive leaders need to engage in a critical conversation detailing roles and how to activate them. This level of communication and advanced planning can facilitate faster decision making and collaboration. Resiliency becomes baked in when cybersecurity becomes a joint capability between the board and executives and through all levels of the organization.

— *Enhancing resilience.* Business continuity answers the question, "How do we operate this process if a particular technology or person is disrupted?" Whereas operational resilience targets the bigger question of, "How do we organize such that a particular event does not disrupt us?" Companies should have answers to both questions to prepare for cybersecurity attacks.

There are quite a few tactical reasons why companies choose to pay, but they all stem from the same underlying concern: we are not confident that this will not disrupt us, so paying is the "safer" option.

Approaching ransomware prevention and preparedness from a resilience perspective frames the requirements and outcomes differently:

— Know what assets are important (crown jewels, critical assets) and where they live. This can not only help assess potential impact in a ransomware attack but also allows for better prioritization and spending policies for infrastructure and security investments.

— Know the backup process, which will help assess how feasible recovery is. It's also good data hygiene to only keep what you need.

— Recovery testing is always helpful. Testing in advance of disruption builds muscle memory, uncovers dependencies, and encourages creative thinking and problem solving.

— Practice—and knowing whether a system will be rebuilt (and how long that will take) or whether systems will failover to an alternate data center—builds confidence in the ability to minimize disruption.

Response

In a ransomware attack, time is of the essence, so collaboration and transparency prevail. When an organization becomes aware of a ransomware attack, it should not compartmentalize the challenges ahead. The CISO or CSO needs to ensure transparency and collaboration with internal stakeholders across the company, including the board, C-suite, affected business groups, compliance and risk, and legal and crisis communications teams. However, your organization's network of external stakeholders can provide valuable input and help expedite risk-based decision making, such as the following:

— *Phone a friend.* An organization's first call should be to the FBI, or a regional and supervisory law-enforcement agency, for notification and disclosure. For very large financial institutions or companies managing and operating critical infrastructure, there is a broad range of law-enforcement capabilities available.

— *Proceed carefully.* The US Department of the Treasury's guidance on ransomware payments requires organizations to consult with them if they need to pay the ransom. However, since ransom payments could violate sanctions against certain individuals or designated organizations, the Treasury's Office of Foreign Assets Control and its Financial Crimes Enforcement Network say organizations could be held liable for ransom payments, even if they were unaware or unable to determine the recipient is on a prohibited list.

— *Seek counsel and check insurance policies.* External counsel, as well as insurers, are significant partners to have at the table. From discerning who to notify and when to working through the finer points of negotiation and

Remember that you are collaborating with criminals, so the closer a company gets to paying the ransom, the more it needs proof that the attackers actually have what they say they have.

possible implications and thinking through the legal requirements for customers and partners—especially third parties—these stakeholders bring practical benefits.

— *Expect pressure.* Some RaaS groups have call centers that will proactively reach out to downstream customers and activist investors to put pressure on a victim to pay. Expect this and have a plan to engage stakeholders, whether proactively or in response to their queries.

— *Activate third-party partners.* Your response leader can serve as "air traffic control" to manage the responsibilities of all parties involved.

— *Dig into forensics and intelligence.* In the earliest stages of the attack, use intelligence to determine who is behind the attack and how they were able to gain access and maintain persistence and detonate the malware. This knowledge will aid in understanding how bad the attack is and assist in decryption and negotiation.

— *Investigate alternatives to payment.* Attempt to locate or access known unencrypted shadow copies of data or even a decryption key using member institution initiatives to determine if their information can be decrypted without paying.

Recovery

No matter what, recovery from a ransomware attack can be messy. If you decide to pay and get a decryption key—and if it works—there is usually a considerable amount of cleanup because the attackers shut down servers and databases not designed to shut down hard. If you don't pay, rebuilding networks from backups is time consuming.

Indeed, the average downtime a company experienced after a ransomware attack is 21 days, according to a Coveware report. In addition, the average ransom fee requested increased from $5,000 in 2018 to about $200,000 in 2020, according to the National Security Institute. But keep in mind, the ransom requested depends on multiple variables like the company size, revenue, industry, and importance.

Also, remember, if an organization suffers an attack and feels it has to pay, the attacker now becomes a business partner, so keep these guidelines in mind:

— *Verify.* For attackers, ransomware is a business, and they want to keep their reputations intact. Remember, however, that you are collaborating with criminals, so the closer a company gets to paying the ransom, the more it needs proof that the attackers actually have what they say they have. Ask to see a sample.

— *Know what's up for debate.* For large and more mature institutions, forensic teams can generally figure out how to find or trigger the decryption key. In these cases, whether or not to pay the ransom depends on the at-risk data elements and how much a company is willing to pay to keep them from being destroyed or exposed.

Make no mistake about it, ransomware is ugly. But making your enterprise resilient by following prevention, preparation, response, and recovery strategies will allow a company to recover from attacks and not have to pay a huge ransom. Communication, advanced preparation, and understanding and then minimizing risk is the best way to keep the operation up and running.

Jim Boehm is a partner in McKinsey's Washington, DC, office, where **Marissa Michel** is a leader, Resilience and Response; **Franz Hall** is a senior adviser in the Stamford office; and **Rich Isenberg** is a partner based in Atlanta.

Designed by McKinsey Global Publishing