Ransomware Protection Best Practices

Harden Your Defenses Now For This Growing Threat

by Chris Sherman and John Kindervag

November 4, 2016

Why Read This Report

Ransomware, once just a consumer scourge, is increasingly holding enterprises hostage. However, by focusing on the basics and implementing proper controls, security and risk (S&R) pros can slow the ransomware snowball. This report explains the rise of ransomware and examines strategies for preventing it — or recovering from it if you become a victim. You will learn best practices to avoid facing an unnerving decision of whether you'll need to negotiate with cyberterrorists.

Key Takeaways

Avoiding Ransom Payment Is Possible

Sometimes it may seem easier to just pay the ransom, but why not mitigate the threat in the first place? With proper backups in place, you can virtually eliminate an attacker's ability to blackmail.

Preventing Ransomware Doesn't Necessarily Require New Security Investments

Ransomware is just malware with an intimidating twist. Your best bet is to optimize your current spending by ensuring that your vendors' solutions provide protection against this threat.

Get Back To Basics: Focus On Your Core Security Needs

It may seem obvious, but you'd be surprised at the contrast between ransomware victims who have addressed their core needs and those who have not. Those who have are in the best position to prevent or recover from ransomware attacks without paying ransom.

Ransomware Protection Best Practices

Harden Your Defenses Now For This Growing Threat

by Chris Sherman and John Kindervag
with Stephanie Balaouras, Christopher McClean, Salvatore Schiano, and Peggy Dostie

November 4, 2016

Table Of Contents

Notes & Resources

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and regulators across industry sectors.

Related Research Documents

Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Core Capabilities

No More Chewy Centers: The Zero Trust Model Of Information Security

Understand The State Of Data Security And Privacy: 2015 To 2016

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Ransomware Uses Desperation As A Primary Means Of Influence

Ransomware has been on the rise in recent years. It's a form of malware that exploits the human element, widespread dependence on electronic data, and the high probability that the targeted victim does not back up their data at all or reliably. Ransomware infiltrates a device, server, network, or other asset and holds it hostage — unable to function — until the victim (an individual or an entire organization) pays a ransom to the anonymous attacker. Often, ransomware locks systems down and prevents users from accessing them altogether; alternatively, ransomware encrypts files on a computer and demands payment to restore the encrypted files. Instead of a steal-and-sell path to monetization, thanks to Bitcoin, criminals can now anonymously receive payment directly from their victim. The result of such an incident on an organization often includes public embarrassment, lawsuits, and a decrease in customer loyalty. If the target is a hospital, the outcome can be a matter of life or death; luckily, the most common outcome we see for hospitals today is a large ransom payment.

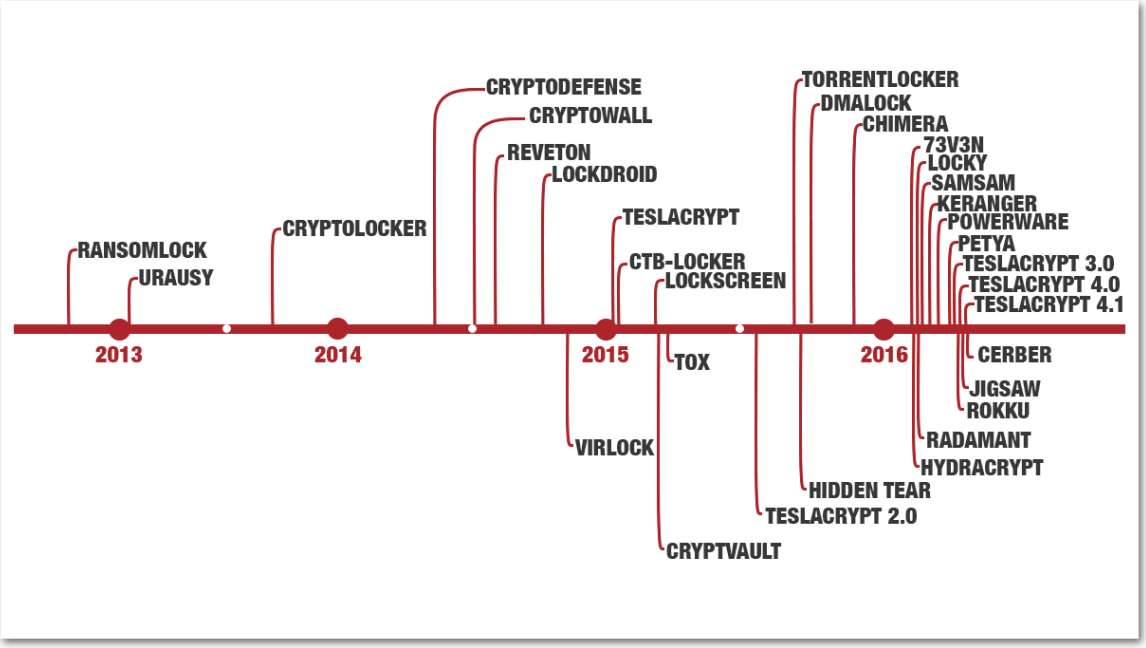
Ransomware Is Skyrocketing Because It's Lucrative And Requires Low Skills

Ransomware makes a lot of sense for hackers; it has an excellent return on investment and takes very little cyberskill, time, or effort for those with the right motivations. It's also been a fundamental business transformation for cybercriminals, who now leverage the power of Bitcoin and take into account user experience. These attacks are increasing because:

- **Individuals are desperate to regain access to critical systems.** Government authorities, healthcare organizations, utility companies, and even individuals have suffered ransomware attacks over the past year.[1] When criminals encrypt data files on your network and demand Bitcoin payment for the key, it leaves critical systems vulnerable to downtime, which can lead to, depending on the industry, an inability to access clean water, power outages, or medical device malfunctions. Earlier this year, the Hollywood Presbyterian Hospital Medical Center's system was infected by ransomware. Before deciding to pay the $17,000 in ransom, administrators were forced to relocate critical patients to local hospitals to ensure medical treatment was not disrupted.[2] Without the proper preventions in place, the only way to regain access to your systems is to pay the ransom, because not even the FBI can decrypt your files.[3] And after paying the ransom, hackers often still delete or steal the majority of your data.[4]
- **Ransomware is more lucrative than your average heist.** Researchers identify new species of ransomware on a rapidly increasing trajectory as criminals react to security practices and devise advanced methods of attack (see Figure 1). The reason for this persistence is likely due to the financial success of cybercriminals deploying ransomware. A 2012 Symantec study found that nearly 3% of compromised users on a command-and-control (C2) server of 5,700 compromised computers paid the $200 ransom.[5] Symantec concluded that criminals profited $33,600 a day from a single C2 server. Keep in mind, ransomware relies heavily on Bitcoin payments; without this anonymous currency, it's too easy to trace the ransom payment back to the criminal.

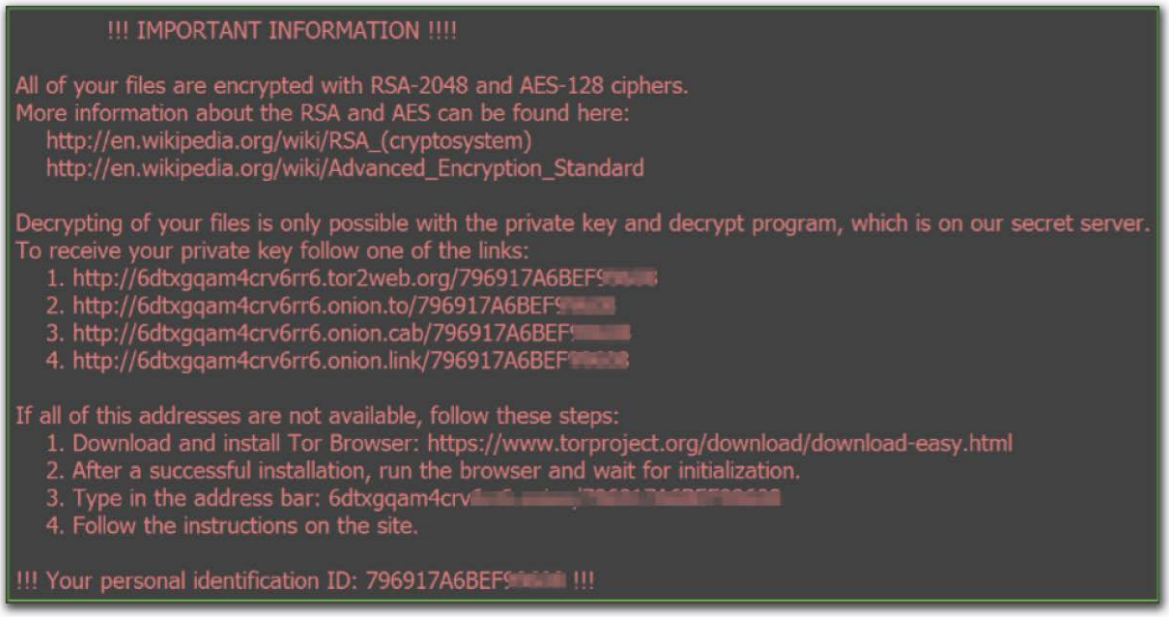
- **Ransomware doesn't take a rocket scientist.** The reality is that new forms of ransomware are relatively easy to launch, regardless of your cyberskill level.[6] Many hackers simply distribute ransomware randomly and wait for the bankroll. Our dark web research has revealed ransomware-as-a-service offered for a small fee, tutorials for social engineering skills, and guides similar to the "For Dummies" series of books, so that even beginners can start a lucrative career. And in 2015, we saw ransomware developed in JavaScript, offered as-a-service on the underground market.[7] Today, anyone with a motive and a dollar can execute (or place an order for) ransomware.
- **Thanks to Bitcoin, a new business model for hackers has emerged.** Traditional hacking monetization has been to steal data and then sell it on the dark net. With the rise of ransomware, we're witnessing a business transformation for the bad guys: They can now skip that last step and, in essence, sell the data right back to the unlucky organization they stole it from in the form of ransom. These criminals still leverage traditional phishing and play on user fears to infiltrate the internal network, but thanks to Bitcoin, they simply freeze the data and anonymously make direct payment demands to the victim.
- **Ransomware criminals understand that a good digital user experience (UX) is key.** Once infected, ransomware implements an easy-to-navigate user experience. The pop-up informs the victim that they've been infected, of course, but it also includes step-by-step instructions on how to make a secure payment and even information on ransomware itself (see Figure 2). "You don't know how to download Tor or upload Bitcoin? It's easy! All you have to do is . . ."

FIGURE 1 Variants Of Ransomware Have Multiplied In Recent Years



Source: Endgame website

FIGURE 2 Ransomware Understands The Importance Of Good UX



Source: Proofpoint website

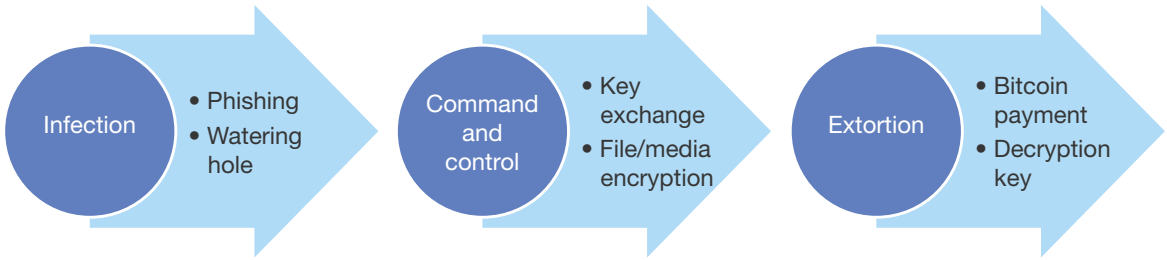
Understand The Simplicity And Effectiveness Of A Ransomware Attack

Ransomware is a new way to leverage existing attack techniques that provide a new path to monetization. And the way it's delivered is no different from the majority of malware: directly to the devices of your unwitting and security-sluggish employees. Therefore, the most appropriate methods of prevention are your tried-and-true techniques. But first, let's boil down ransomware to three simple steps (see Figure 3):

- **It starts with an infection of ransomware malware.** Ransomware spreads in the same manner as most malware. It targets victims through phishing and watering-hole attacks. These types of attacks are well understood, and there are mature and effective exiting countermeasures. The rise in ransomware malware may indicate that security teams have not widely deployed these controls or may signal a significant configuration issue in the tools.
- **Then there is a connection to C2 infrastructure.** Attackers frequently use command-and-control infrastructure to exchange encryption keys with the host system and issue demands to their victims. For a key exchange to successfully happen, the malware must be able to connect with the ransomware servers.

› **Cybercriminals demand ransom to unencrypt or grant you control of your data again.** Because of Bitcoin, the hacker business model has evolved. Instead of having to actually steal data and sell it underground, criminals can still get paid the big bucks by merely threatening to do so. They simply demand an anonymized Bitcoin sum directly from the victim in exchange for a decryption key to the victim's recently encrypted files.

FIGURE 3 The Basics Of Ransomware



The Most Common Targets For Ransomware Are Your Employees' Devices

Of course, ransomware facilitators aren't simply after your employees' vacation pictures; the goal is to freeze critical operational data and systems and urge you to pay up. The route hackers take to get to this finish line is to target weak points of your network, namely company-owned and employee devices. More specifically:

› **Personal computers' OSes make up the bulk of all ransomware attacks.** The majority of personal computers that are targeted run the Windows operating system, although recently we have witnessed ransomware on OS X.[8] Ransomware targets OSes to leverage system API hooks and block access to controls such as the mouse and keyboard. Many crypto variants actually make use of native encryption libraries or APIs supplied with the OS — to save attackers the trouble of inventing their own encryption method.

› **Mobile phones and tablets are the second-most-targeted types of devices.** Android and iOS are the two primary OSes for mobile. It's much more difficult for criminals to attack nonjailbroken iOSes, but this is changing quickly.[9] As a more open and permissive platform, Android is attractive and now makes up over 80% of the mobile market. Just recently, Symantec noted that two-thirds of Android users are vulnerable to Lockdroid ransomware, a variant that holds a user's browsing history for ransom.[10] Because mobile devices have historically been meant more for messaging and leisure activities, attackers see less value there, and the majority of ransomware for mobile to date has been experimental. However, as we continue to use mobile for payments, banking, and work email and data storage, we expect to see ransomware advance for mobile devices.

› **Servers are more likely to contain critical data.** Servers act as central repositories for enterprises, making them high-value targets, although less often targeted. Attackers typically demand 10 to 50 times more money to decrypt a server. Server targets are often combined with DDoS attacks to blackmail businesses. Some attackers infiltrate the server and patch the software so that the stored data is encrypted, along with all of the backups. Once enough backups are encrypted, criminals make their ransom demands, which are typically much more aggressive compared with smaller targets

› **Wearables and IoT devices will become future targets.** In 2015, we predicted that we'll see ransomware for a medical device or wearable in 2016.[11] Unfortunately this came true early in 2016 and will likely increase in prevalence as the number of IoT devices within healthcare continues to increase.[12] Connected cars, wearables, implantable medical devices, home automation — the internet of things is increasing the attack surface, creating more ransomware targets for creative criminals. A future where you can get locked out of your new car until ransom is paid by the manufacturer is not far-fetched.[13]

You Have The Tools To Mitigate Ransomware

Classic hacking methods such as social engineering, phishing, and malvertising work well for hackers, so why change what's already working? In fact, ransomware exposes weaknesses in basic best practices that should already be in place inside all enterprises. One of the best ways to look at the issue of ransomware is through a problem/solution lens. To mitigate the problem of ransomware, focus on five essential solution statements.

No. 1: Protect Against Known Ransomware Vulnerabilities

Ransomware often exploits known vulnerabilities within endpoint applications, web browsers, and web pages in the initial stages of their attacks. Harden your defenses against the known vulnerabilities before putting effort into detecting the subsequent stages. We recommend that you:

› **Correlate exploits to vulnerabilities, and prioritize patching.** Ransomware uses a small subset of vulnerabilities to be effective, but security researchers have been able to identify those vulnerabilities. Therefore, an immediate step for every security team is to identify the vulnerabilities in your organization and to begin prioritizing patches. Before you prioritize patching, first understand what's going on and how it affects your organization. Look at the vulnerability management life cycle — validate, discover, assess, report, and remediate — to discover what vulnerabilities you have.

› **Work with a vulnerability management vendor to scan and patch.** Security teams must constantly scan for vulnerabilities in the organization. It's important to ensure the scanner is always up to date. If you don't know what's vulnerable and could lead to ransomware, how are you going to know what to patch? For example, a major vulnerability right now is Silverlight, which runs a

remote code execution. Once identified, you should patch and correlate this information while consistently scanning for more so that you can prioritize the right patches. If you don't do this, ransomware will find and take advantage of the vulnerabilities in your organization.

› **Assign patch priority based on P3 scores.** After you've decided on the risk classification scales and weightings most appropriate to your IT operations requirements and risk appetite, you must determine patch criticality based on the three measurements of Forrester's prioritized patching process (P3).[14] Data classification tools will help you understand what data you have and how to classify it by application data sensitivity: toxic (the highest sensitivity level), internal, or public.[15] Next, a predictive threat model will allow you to anticipate the attack difficulty.[16] And last, a third-party vulnerability management vendor will work with you to assess and classify vulnerability intrinsic risk.[17] Once each missing patch within an organization has an associated P3 score, you can prioritize their testing and remediation efforts in a much more pragmatic and efficient manner.

No. 2: Protect Against Phishing And Watering Hole Attacks

Attackers must find a way to inject malware into your networks and systems. One of the most foolproof ways is to use phishing email links or malicious websites known as watering holes to route traffic to sites that will automatically download and install ransomware to machines. As ransomware becomes more sophisticated, cybercriminals have shifted from spam email to spear phishing, targeting specific individuals in your network.[18] Unfortunately, phishing attacks are the most difficult to prevent. Distressing messages will then appear (some even pretending to be the FBI), locking the user out and exclaiming that the user has broken the law, demanding ransom to give back control of the computer (see Figure 4). Through social media, attackers identify employees and send them personalized emails, increasing their chances of clicking on a malicious link or downloading a malicious file and granting permissions. To mitigate this risk, we recommend that you:

› **Leverage antispam, phishing, and web control tools for employee protection.** Although your employees are capable, motivated people, every CISO knows it's nearly impossible to get them to be proactive about security. And it's not their fault. You must ensure the proper protections are in place.

› **Encourage the human firewall.** The human factor involved in ransomware attacks is undeniable. Look no further than the Klinikum Arnsberg hospital in Germany: The ransomware infection was traced back to a booby-trapped email unwittingly opened by an employee.[19] You'll never be able to eliminate this human vulnerability, but you can mitigate it to the best of your ability. It's all too easy for users to download a malicious file or click on the wrong link, especially when the email is personalized. And it's not the employee's fault; attackers leverage social media to target or imitate employees. Train staff in a manner that explains why you're doing the training; employees are more understanding and motivated if they get it.[20]

› **Don't blame the victims; instead, give them the right tools.** You should never blame your employees for interacting with a malicious email or link. Regular security training should absolutely be a requirement, but for complete email threat protection you must deliver a comprehensive set of capabilities. These include: 1) antispam; 2) categorization of graymail; 3) robust static and dynamic analysis tools; 4) URL rewriting; and 5) analytics to prevent phishing and email fraud.[21]

FIGURE 4 Example Ransomware Notification

Source: Bleeping Computer website

No. 3: Protect Against Malverstisements And Downloaders With Proper Endpoint Protection

Malvertisement and downloaders are also efficient tools for spreading ransomware. Malicious advertisements are frequently used to exploit browser vulnerabilities in order to serve and install ransomware. For example, in January 2015, attackers implanted ransomware on ads served by AOL's

ad network that affected ads on sites such as The Huffington Post and men's magazine FHM.[22] Your endpoint security solution must be equipped with the right tools to prevent and detect ransomware threats originating from web, email, and local sources. We recommend that you:

- **Go beyond traditional blacklist-based endpoint security for maximum protection.** Don't rely on outdated controls on the endpoint to stop modern variants of ransomware.[23] Effective endpoint security is critical to defend against ransomware; this starts with balancing strong malware prevention with behavioral detection capabilities.[24]
- **Focus on attack surface reduction.** Build up your endpoint defenses by decreasing your attack surface available to ransomware.[25] Consider implementing a default-deny whitelisting policy to limit your exposure to zero day ransomware variants. For even stronger protection, enforce a least-privilege access policy by removing endpoint admin rights and escalating on a per-app basis.[26]
- **Detect and block malicious behavior.** Despite the best-laid plans, ransomware will eventually get past preventive controls. This is why it's crucial to have proper detection-focused tools in place to catch and block malicious process behavior. When evaluating your existing investments (or potential new ones), make sure running memory behavior is analyzed; with the advent of fileless ransomware, it's important to go beyond static file scanning offered by most antimalware engines. Also keep an eye on products with automatic containment that detect, block, and then remediate without admin involvement. If a solution requires a skilled security analyst to make convictions on alerts after a compromise occurs, it will likely be too late.

No. 4: Ensure That The Right Network Level Protections Are In Place

For cybercriminals to successfully install malware inside of your network, the actual malicious software must travel across your network. Your network may not have the right controls in place or your policies may not be restrictive enough to stop malware. Network security controls will ideally block ransomware attacks before they reach the endpoint. We recommend that you:

- **Beef up your network security controls to allow only known-good traffic.** Most enterprises allow a great deal of malicious traffic into their network because they're afraid of stopping good or legitimate business traffic. This hypersensitivity allows false positives into the soft underbelly of network security. Security teams should adopt the Zero Trust Model of information security, which will drive policies that drop much of the maliciously embedded traffic before it can even enter your network.[27] The United States House of Representatives recently recommended a Zero Trust approach for all US federal government networks in the wake of the disastrous Office of Personnel Management (OPM) breach.[28]
- **Deploy next-generation firewalls (NGFWs).** This modern take on the firewall combines multiple controls into a single platform in order to make network security management more efficient. One significant feature is the ability to look at the entire packet all the way through layer 7. Make sure that NGFW rules are written to take advantage of layer 7 inspection.

› **Deploy a solution for automated malware analysis (AMA).** AMA controls run unknown attachments coming into your network inside of a sandbox to see if they're malicious. These tools can be effective, but their policy must be set properly. Many security teams are so afraid of stopping good attachments that they allow malware containing attachments to pass through to their destination while the sandboxing occurs. The idea is that they can alert that a potential piece of malicious software has come into the network, but with the rise of ransomware and other malware variants, this methodology is too late. Set up your AMA gateways so that they test every attachment to make sure it's clean before being delivered to its destination.

No. 5: Bulletproof Your Backup And Recovery Practices

Many small and medium-size businesses back up their data infrequently or not at all. Even at the enterprise level, backups are problematic. Backups complete at a 95% or higher success rate, which sounds impressive until one realizes that most complete with errors that administrators never have enough time to investigate, diagnose, and resolve. In addition, even at the enterprise level there are gaps in backup coverage. Many enterprises don't have a centralized policy for backing up laptops or remote offices. Ransomware attackers depend on the fact that you don't have a recent and successful backup from which to restore and that said backup is clean — meaning the backup itself isn't already infected with the malware. If victims have recent and available backups, they can restore data and ignore extortion demands. We recommend that you:

› **Focus on frequent and clean backups.** To defeat ransomware with backups, focus on two significant areas: frequency and cleanliness. Ransomware is effective if companies don't have backups that are recent enough to restore data and keep the business running. Additionally, it should be noted that the backup must be clean. This means that the malware has not already infected the device, which will transfer the malware to the backup, and restoration will lead to new ransomware infections.

› **Schedule frequent backups.** Out of the hospitals that have been hit with ransomware attacks, those that avoided paying ransom were the ones with solid data backups.[29] It's true! Cybercriminals can't hold your data hostage and extort you for ransom if you have another copy of it. Work with your infrastructure and operations counterparts to build and implement a backup and disaster recovery plan.[30] Just make sure that once you've implemented it, you're testing it frequently and using a variety of test types.[31]

› **Watch backups for malware.** Make sure that you know that a machine or device is not currently infected with malware before backing it up. For example, automated file sync solutions may not be an effective backup method because the malware will be immediately synced and the whole backup will be infected. File synchronization solutions are powerful and important, but they should not be used as a replacement for more traditional backup solutions.

Recommendations

Focus On Your Core Security Maturity To Reduce Ransomware Risks

Fighting ransomware doesn't require a fancy new tool; it does, however, require a focus on the core needs required for defending your environment against targeted attacks so that you can lay a foundation for a resilient security strategy. The first four basic needs of Forrester's ransomware targeted-attack hierarchy are: 1) an actual security strategy; 2) a dedication to recruiting and retaining staff; 3) a focus on the fundamentals; and 4) an integrated portfolio that enables orchestration. The second two — 5) prevention and 6) detection and response — will fail if you haven't first established the core four. Today's needs for detection and response include: malware analysis, network analysis and visibility, endpoint visibility and control, and security analytics. If you focus on this hierarchy, you will compel your organization to adopt a strategy to mitigate the threat of ransomware.

Endnotes

[1] A Michigan electricity utility was taken down by ransomware attack earlier this year. Source: Richard Chirgwin, "Michigan electricity utility downed by ransomware attack," The Register, May 3, 2016 (http://www.theregister.co.uk/2016/05/03/michigan_electricity_utility_downed_by_ransomware_attack/).

Personal ransomware attack targets 100 million people. Source: Kevin Downey, "New sophisticated ransomware attack targets 100 million people," Kim Komando, May 26, 2016 (http://www.komando.com/happening-now/360662/new-sophisticated-ransomware-attack-targets-100-million-people).

Source: Jack McCarthy, "MedStar attack found to be ransomware, hackers demand Bitcoin," Healthcare IT News, April 4, 2016 (http://www.healthcareitnews.com/news/medstar-attack-found-be-ransomware-hackers-demand-bitcoin).

[2] Source: Kaveh Waddell, "A Hospital Paralyzed by Hackers," The Atlantic, February 17, 2016 (http://www.theatlantic.com/technology/archive/2016/02/hackers-are-holding-a-hospitals-patient-data-ransom/463008/).

[3] Source: "Ransomware on the Rise," FBI, January 20, 2015 (https://www.fbi.gov/news/stories/ransomware-on-the-rise).

[4] Source: Interview with an anonymous managed service provider.

[5] Source: "Ransomware: How to Earn $33,000 Daily," Symantec Security Response, November 8, 2012 (http://www.symantec.com/connect/blogs/ransomware-how-earn-33000-daily).

[6] A fully functional ransomware code was posted on GitHub by a Turkish security researcher. Source: Khyati Jain, "Script Kiddies can Now Create their Own Ransomware using This Kit," The Hacker News, August 18, 2015 (http://thehackernews.com/2015/08/ransomware-creator-toolkit.html).

[7] Source: Pierluigi Paganini, "Analyzing Ransom32, the first JavaScript ransomware variant," Security Affairs, January 3, 2016 (http://securityaffairs.co/wordpress/43250/cyber-crime/ransom32-crypto-ransomware.html).

[8] Source: Claud Xiao and Jin Chen, "New OS X Ransomware KeRanger Infected Transmission BitTorrent Client Installer," Palo Alto Networks, March 6, 2016 (http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/).

[9] According to Kaspersky Labs, from 2010 through 2014, malware targeting OS X increased 3,600%. Source: Eugene Kaspersky, "The evolution of OS X malware," Nota Bene: Eugene Kaspersky's Official Blog, September 29, 2014 (https://eugene.kaspersky.com/2014/09/29/the-evolution-of-os-x-malware/).

Source: Swati Khandelwal, "First MAC OS X Ransomware Targets Apple Users," The Hacker News, March 6, 2016 (http://thehackernews.com/2016/03/mac-os-x-ransomware.html).

[10] Source: John Leyden, "Two-thirds of Android users vulnerable to web history sniff ransomware," The Register, January 29, 2016 (http://www.theregister.co.uk/2016/01/29/android_ransomware/).

[11] For more of our 2016 predictions, see the "Predictions 2016: Cybersecurity Swings To Prevention" Forrester report.

[12] In February 2016, Hollywood Presbyterian Medical Center reported that attackers had disabled a number of medical devices such as CT scanners in an ongoing ransomware attack. For more information on the risks within healthcare and IoT, see the "Healthcare's IoT Dilemma: Connected Medical Devices" Forrester report.

[13] An article from last year outlines some of the new threats posed by connected cars. Source: "Connected cars: The dangers posed by hackers," IDG Connect, July 7, 2015 (http://www.idgconnect.com/blog-abstract/10144/connected-cars-the-dangers-posed-hackers).

Security researchers have successfully hacked a car and were able to turn it off mid-ride; this article explains some ways it could be even worse. Source: Andy Greenberg, "The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse," Wired, August 1, 2016 (https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/).

[14] Forrester has defined a new scalable process that we call the prioritized patching process (P3, for short). Our contextual approach to prioritization requires business value analysis married with detailed knowledge of the environment and predictive threat modeling. For more on this process, see the "Introducing Forrester's Prioritized Patching Process (P3)" Forrester report.

[15] For our analysis of the data loss prevention market, see the "Market Overview: Data Loss Prevention" Forrester report.

[16] For our analysis of the 15 technologies that comprise the most important network threat mitigation technologies, see the "TechRadar™: Zero Trust Network Threat Mitigation Technology, Q1 2015" Forrester report.

[17] Cybersecurity incident disclosures and vulnerability warnings continue to be released at an alarming and fatiguing rate, and there aren't any signs of breach activity slowing down. Vulnerability management is more important than ever, yet staying on top of vulnerabilities poses a major challenge for security and risk (S&R) professionals. For more information, see the "Market Overview: Vulnerability Management" Forrester report.

[18] For more information, see the "Four Ways Cybercriminals Exploit Social Media" Forrester report.

[19] Staffers detected the malware on one of the hospital's 200 servers before pulling the plug. Source: Sarah Steffen, "Hackers hold German hospital data hostage," Deutsche Welle, February 25, 2016 (http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030?maca=en-rss-en-all-1573-rdf).

[20] The human element is one of the most critical aspects of your security program, yet it's often the most neglected. Many security leaders prioritize other projects and see little value in the efforts they do commit to training and awareness. However, this is the problem: Awareness initiatives are sporadic, with materials that reflect the minimal, uninspired investment. To learn more, see the "Reinvent Security Awareness To Engage The Human Firewall" Forrester report.

[21] For more information, see the "Brief: Five Key Capabilities For Microsoft Office 365 Email Security" Forrester report.

[22] To learn more about these types of attacks, see the "Brief: Protect Employees And Customers From Malvertising" Forrester report.

[23] As malware increases in sophistication and the number of new variants rises, antivirus (AV) technologies have steadily become less effective at stopping advanced threats to employee endpoints and servers, and security and risk (S&R) professionals have begun to realize this, as evidenced by survey results showing decreased adoption and interest in AV among small and medium-size businesses and enterprises alike. A growing number of S&R pros are considering replacing their third-party AV tools with native (OS) AV augmented with one or more of the following third-party AV alternatives: application whitelisting, application privilege management, application integrity protection, endpoint execution isolation, and endpoint visibility and control. For more information, see the "Prepare For The Post-AV Era Part 1: Five Alternatives To Endpoint Antivirus" Forrester report.

[24] Every year, Forrester surveys thousands of security decision-makers and information workers globally from a wide range of industries and organization sizes. This report presents the most relevant endpoint security data from these surveys, with special attention given to trends affecting small and medium-size businesses and enterprises. To learn more, see the "The 2016 State Of Endpoint Security Adoption" Forrester report.

[25] To learn more, see the "Best Practices For Securing And Empowering A Mobile Workforce" Forrester report.

[26] In this second report covering the post-antivirus (AV) era, we discuss how a layered approach to endpoint security can help decrease the risk of attack significantly beyond what antivirus alone can achieve. A growing number of security professionals are considering replacing their third-party AV tool with one or more alternatives to traditional blacklist-based virus protection, but nothing available today offers protection broad and deep enough to cover all potential avenues for attack on the endpoint. To learn more, see the "Prepare For The Post-AV Era Part 2: Layer Your Endpoint Security Tools For Max Protection" Forrester report.

[27] There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For today's digital business, this perimeter-based security model is ineffective against malicious insiders and targeted attacks. Security and risk (S&R) pros must eliminate the soft chewy center and make security ubiquitous throughout the digital business ecosystem — not just at the perimeter. In 2009, we developed a new information security model, called the Zero Trust Model, which has gained widespread acceptance and adoption. To learn more, see the "No More Chewy Centers: The Zero Trust Model Of Information Security" Forrester report.

[28] Source: Erin Kelly, "Feds must have 'zero trust' of employees to stop hackers, report says," USA Today, September 7, 2016 (http://www.usatoday.com/story/news/politics/2016/09/07/feds-must-have-zero-trust-employees-stop-hackers-report-says/89947108/).

[29] Staffers detected the malware on one of the hospital's 200 servers before pulling the plug. Source: Sarah Steffen, "Hackers hold German hospital data hostage," Deutsche Welle, February 25, 2016 (http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030?maca=en-rss-en-all-1573-rdf).

[30] Infrastructure and operations (I&O) leaders have a growing number of services and tools to better prepare themselves for any type of event, whether it's natural or man-made; however, that doesn't mean that enterprises are able to recover with the minimal data loss and downtime that the business demands. The benchmarks found in this report are the result of several years of market studies on business continuity and disaster recovery developed in partnership with Forrester and the Disaster Recovery Journal. Specific benchmarks include process maturity, adoption of cloud and colocation disaster recovery sites, adoption of advanced recovery time and recovery point capabilities, top reasons for organizational downtime, and the driving forces behind improved DR capabilities. For more, see the "The State Of Business Technology Resiliency, Q2 2014" Forrester report.

[31] During the busy holidays, there is always news of a website breach or crash. Despite the millions of dollars they generate for their businesses, websites remain vulnerable to cyberattack, performance issues, and unplanned downtime — but they don't have to be. To learn more, see the "Seven Steps To Protect Your eCommerce Website In 2016" Forrester report.

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.