AXA

XL Insurance

Ransomware: A clear and present danger

Insights and best practices to keep your business moving forward

co-authored by

S-RM

Introduction

Since its emergence onto the cyber landscape in 2012, ransomware has become a clear and present danger to organizations' business operations worldwide. With a string of high-profile incidents impacting a number of Fortune 100 companies such as FedEx and Merck, and a projected global price tag of $11.5B in 2019, ransomware is rightfully considered one of the most significant cyber risks to organizations of all sizes. Ransomware impacts manifest on multiple fronts, whether it be a grinding halt to business operations, reputational damage, or the considerable financial impact associated with restoring systems and operations. In this article, we explore:

- The tools cyber criminals use to distribute and monetize ransomware
- The ability of authorities to enforce cyber laws globally
- Historical, current, and future ransomware trends
- Ransomware's total impact
- Best practices to prevent, mitigate, detect, and respond to a ransomware attack

Cyber crime and enforcement of cyber laws

According to research by Trustwave, the return on investment ("ROI") from ransomware campaigns can be as high as 1400%.

Tools of the trade: Distributing and monetizing ransomware

Ransomware, as its name implies, is a form of malware that literally holds an organization's data hostage. By encrypting critical files, ransomware renders systems inoperable, crippling IT and business operations. Cyber criminals monetize this type of malware by demanding payments to decrypt the data, a method akin to a kidnapper releasing a hostage for a ransom payment. As with traditional kidnapping, many victims see paying the ransom as the path of least resistance, and the choice that will most likely get their data decrypted and their operations up and running again. The most common initial vector for ransomware infection is social engineering via email. A seemingly legitimate email tricks its recipients into executing the ransomware and triggering its spread throughout the network. In other notable cases, ransomware infections were caused by browsing malicious websites or using an infected USB thumb drive.

There's no lack of business acumen amongst cyber criminal groups. While many of these groups launch their own coordinated ransomware attacks, some of them also launch these attacks on behalf of others as part of a managed service. As such, we've seen the rise of Ransomware-as-a-Service ("RaaS"), a managed service offered by cyber criminal groups that includes personalized access to a platform to distribute ransomware, as well as technical support and dashboarding capabilities, for a fee typically collected in cryptocurrency. This means that nearly anyone with internet access, regardless of technical knowhow, can launch a ransomware attack against a target of their choice with minimal effort. According to research by Trustwave, the return on investment ("ROI") from ransomware campaigns can be as high as 1400%. With such an astronomical return, one can imagine how incentivized criminal elements are in conducting ransomware campaigns.

The rise of cryptocurrencies has played a prominent role in cyber crime. While cryptocurrencies have many legitimate use cases, their reputation for anonymity and difficulty to trace have made them ideal currencies for cyber criminals. Whether it be paying the fees for a RaaS platform, or collecting a ransom payment, cryptocurrencies have played a fundamental role in the rise of ransomware in the cyber threat landscape. The most popular of these cryptocurrencies, Bitcoin, is explored next.

Cybercrime financed by bitcoin

Bitcoin is the preferred currency for ransoms. Cyber criminals use Bitcoin primarily because transactions can be very difficult to trace to a person and because it remains the most accessible cryptocurrency available. While it is difficult to connect a person to a Bitcoin transaction, paradoxically, all Bitcoin transactions are documented in a public ledger that can be viewed online. This allows a cyber criminal to know in real-time when clients make ransom payments so that they can act accordingly, streamlining their operations.

However, the sense of anonymity that comes with using Bitcoin may be misplaced due to the public nature of the system. Because all transactions are public, digital forensic experts can trace the lifecycle of a given Bitcoin and have had success in tracing these payments to individuals, usually by using sophisticated graph mapping algorithms to infer the identity behind a bitcoin address, or by using other methods to reveal identity when attempting to convert Bitcoins into fiat currency, i.e. cash. In the US for example, every major Bitcoin exchange is regulated by the Financial Crimes Enforcement Network (FINCEN), and therefore, any person attempting to convert Bitcoins into fiat currency at an exchange should be identifiable. However, like other money laundering schemes, criminals will find ways around the rules, especially in jurisdictions with less regulation.

As an example, in 2015, two rogue federal agents from the Drug Enforcement Administration (DEA) and the Secret Service were arrested and convicted on various charges related to the theft of Bitcoins seized from a dark web market. Federal agencies had traced the Bitcoin transactions in the public ledger, tying them to the two agents, using methods that have not been publicly disclosed. There have been several other recent examples where law enforcement has successfully traced cyber criminals using the same method. Apprehending these criminals, however, is an entirely different matter, and we explore the agencies' abilities to enforce laws meant to protect us from ransomware cybercrime in the next section.

Enforcement of cyber laws

Unmasking the identities of cyber criminals is one thing; apprehending them and having them face the letter of the law is an entirely different animal. Oftentimes, cyber criminal groups operate in different geographical areas under the jurisdiction of different laws. For example, one of these groups could have members operating in the US, various European countries, and Asian countries simultaneously. Unmasking all these actors and apprehending them takes an enormous amount of international cooperation and coordination amongst law enforcement agencies. While that may be feasible between allies and other countries with friendly relations, it may be an impossible feat in other circumstances where legal frameworks between countries have not been defined, or worse, where diplomatic relations barely exist.

In one case, in September 2018, the Department of Justice (DOJ) charged Park Jin Hyok with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions for the role he allegedly played in some of the highest profile cyber attacks in recent history. As a prominent member of the infamous, and suspected North Korea-sponsored, "Lazarus Group" hacking collective, Park was implicated in: 2017's Wannacry 2.0 ransomware campaign, the $81M cyber heist from the Bangladesh Central Bank, and the 2014 Sony breach. However, while identified and charged, the DOJ has limited enforcement capabilities in this case because Park is a North Korean citizen suspected to be living in China. Enforcement against Park would be extremely difficult, as China lacks an extradition treaty with the US and other western countries.

Ransomware's total impact

The state of ransomware

Ransomware attacks have indiscriminately targeted consumers and enterprises globally. According to Symantec, in 2018, the countries with the most ransomware infections were China (17%), India (14%), and the US (13%). Mobile ransomware infections also have a global spread, with the US, China, and Germany accounting for 63%, 13% and 10%, respectively.

The first forms of ransomware can be traced back to 1989 when the AIDS Trojan was circulated on 5 ¼" floppy disks sent via post mail. However, it wasn't until 2012 that ransomware began using encryption to disable its victims' systems. Prior to 2012, ransomware utilized other, less crippling methods to convince its victims to remit payment to attackers. Given ransomware's underground success, it is now the most common form of malware in circulation. Encryption is widely used to keep our sensitive data private, but now it has been weaponized and used against us by holding data hostage for ransom. In the current information age, data fuels our economies and cyber criminals want a piece of the pie. Historically their tactics included stealing information and selling it to the highest bidder on dark markets and other covert channels, but since then they've realized a more profitable venture using 21st century extortion. It should come as no surprise that cyber criminals continuously change their tactics in order to maintain their revenue streams, but what is surprising is how they continue to identify and creatively exploit vulnerabilities. In and out of cyberspace we continue to see criminals weaponize familiar tools and use them to their advantage, harkening back to 9/11 when we first saw airplanes used as weapons of mass destruction.

Today, ransomware is a nightmare for IT and security professionals. Even with reputable security technology in place, organizations are still experiencing ransomware infections, resulting in disrupted operations, damaged reputations, and costing billions of dollars globally. It wasn't long ago that ransom demands of $50,000 were considered high; today we are seeing ransom demands over $2MM. Recent widespread infections have included Ryuk, Samas/SamSam, and Dridex ransomware strains. During ransomware's infancy, cyber ransoms were not particularly high because large ransom demands attract law enforcement attention. **Globally, ransom demands have soared from $1BN in 2016 to $11.5BN in 2019**. This increase can likely be attributed to the rate at which organizations are paying the ransoms. In many cases, the cost of paying a ransom is less than the expected business interruption cost. This is especially true when a ransomware infection results in loss of unrecoverable revenue. In addition, organizations are increasingly investing in Cyber insurance coverage, which usually covers the cost of cyber ransom payments.

Given these developments, it makes sense that organizations are seeing targeted attacks that are 4.5 times the number of the opportunistic attacks that consumers receive, according to recent research from Symantec. Opportunistic attacks are usually generic so that they can be used against a wide audience, but generally have a lower success rate because they are easier to identify and prevent. Targeted attacks are usually tailored to a specific audience or organization and are intended to extract significantly more money from each operation.

So which types of organizations are being targeted? In the next section, we explore ransomware's most frequently targeted victims.

Common ransomware victims

As cyber criminals begin to shift to more targeted ransomware campaigns in an attempt to extract more money from their victims, they are focusing on three organization types:

- those that have a direct correlation between technology uptime and revenue generation
- those that have a significant impact on health and safety
- those that are unprepared

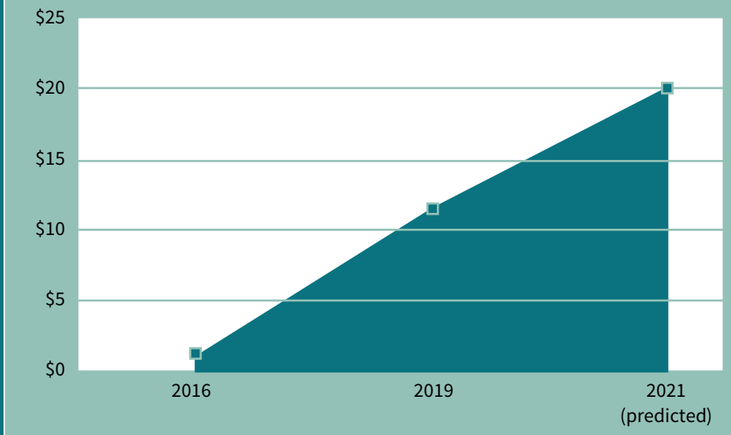
Countries with the most ransomware attacks
Symantec, 2018

17%
China

14%
India

13%
United States

Global Ransomware Extortion Payments
(Estimated in $B)



It wasn't long ago that ransom demands of $50,000 were considered high; today we are seeing ransom demands over $2MM.

Targeted attacks are usually tailored to a specific audience or organization and are intended to extract significantly more money from each operation.

A targeted ransomware attack usually victimizes organizations that rely heavily on technology, in which downtime would have a direct impact on revenue, especially where such uncollected revenue would be unrecoverable. Today, many organizations fit this description, but those hit the hardest would include retail, utilities, financial services, and manufacturing. In a retail environment, for example, an outage affecting checkout would likely send customers to a different retailer to make their purchases, resulting in lost opportunities. In manufacturing, most companies run their production equipment close to full capacity in order to maximize their machinery investment. In both examples, downtime has a direct impact on revenue that can't be recovered.

However, it isn't just revenue generation that is targeted. As we've seen with ransomware attacks against healthcare companies, the decision to pay a ransom might not be a business decision, but rather a health and safety decision. A ransomware attack on a health organization could have life or death consequences, and cyber criminals know this is another vulnerability that can be exploited.

Many low-margin organizations inherently struggle to find enough resources to properly protect themselves from the ransomware threat. Because they are unprepared, many are left with no options; they must either pay the ransom or start over. Non-profits, municipalities, and other small businesses are targeted by ransomware because many of them are not able to obtain the budget needed to properly defend against ransomware risks. While it may be a significant financial burden for some organizations to invest in the right defenses for ransomware, the total impact of a widespread infection is likely much more significant. In the next section, we explore other impacts to consider.

Considering the total impact

Having worked many ransomware response cases, we have found that many of our clients were not prepared for the complexity and cost of the response, even when the incident was resolved by paying the ransom. In the following sections we identify each response element and some tips to keep in mind as you consider your current incident response capabilities and if the terms of your Cyber insurance policy sufficiently address ransomware risks.

Ransom payment

Consider the following: If your organization made the decision to pay a $1MM ransom in Bitcoin, how would you do it? If you haven't purchased and transferred $1MM worth of Bitcoin in the past, you might be surprised by the complexity of the process and the amount of risk involved in the transaction. The good news for those with Cyber insurance is that Cyber ransom payments are typically handled on the insured's behalf by a trusted third party. Keep in mind that most Bitcoin exchanges have maximum purchase limits of $20,000 or less per day. Assuming you don't have 50 days to waste maxing out your purchase limits, you will likely need to engage a third party to make the payment on your behalf. These payments often carry heavy fees to cover the administration and overhead associated with making ransom payments to criminal organizations.

Beyond the primary challenges associated with acquiring Bitcoin, there are many other risks to consider. For example, Bitcoin transactions cannot be reversed and are not managed by a central authority. Bitcoin payments are made using a Bitcoin address that is formed by a long string of letters and numbers. There is no error handling when addressing a Bitcoin payment, so if one character is out of place, the payment will not make it to the intended party, and the misaddressed Bitcoin is likely irretrievable. In addition, we have seen hackers attack Bitcoin transactions and reroute them to their own Bitcoin wallets. Also, when making a ransom payment, you must consider the legality of your payment, especially if you've been attacked by a sanctioned group, such as a Foreign Terrorist Organization (FTO). There are laws and regulations that may govern your ransom payment. Your Bitcoin payment provider of choice should help you navigate these complexities.

Forensics

Many assume that a good forensic investigation will answer any questions that may come up during and after an incident. In fact, the success of a forensic investigation relies on having the right information available to analyze. This requires the right mix of technologies that are properly configured to produce an accurate account of events, many times in the form of audit logs. Many organizations that go through a forensic investigation for the first time find that they could have improved outcomes if their logs captured more useful information and if they handled forensic evidence, such as temporary data stored in memory, more carefully. Also, many times breaches are discovered months or years after they occurred, which may be beyond the retention period for some organizations. Without good forensic evidence to analyze, an organization will have a very difficult time knowing what information has been breached, and therefore will likely assume the worst, resulting in a much costlier response.

Legal

The legal response to a ransomware attack can be dizzying considering that each state has their own breach notification laws; even the simple definition of a data breach is not consistent between states. Typically, a forensic investigation is needed to determine which legal requirements have been triggered. In many cases, ransomware is not intended to impact data confidentiality; instead, its goal is to make data unavailable. Many state data breach laws define a data breach as an unauthorized acquisition of personal data, but others define it as unauthorized access to protected data. Without knowing more about the specific infection, it isn't possible to determine if a breach has occurred. In some cases, a ransomware incident might not be considered a breach, if, for example, it is clear that protected data wasn't exfiltrated, or if the affected data was encrypted and hadn't been decrypted by the attackers. Given all of these complexities, breach notification is typically a specialized field where employing expert legal counsel is critical.

Public Relations/Crisis Communications

Once a breach becomes public, it's likely that staff won't be able to handle the influx of inquiries from affected parties and the media. Outside help is needed, and warranted, so that the situation remains manageable. It is important to have control over the messaging, and a reputable public relations agency can help craft and deliver it. Large breaches may require a dedicated call center to field calls from affected individuals.

Business Interruption

While it is true that ransom demands continue to increase, and quite drastically in some cases, we often find that the associated business interruption costs and associated reputational damage far exceeds the ransom demand. In fact, organizations that are vulnerable to these impacts are much more likely to be targeted by the groups that perpetrate these crimes. In a complex business environment, a formal business impact analysis may be required to understand what business interruption will cost the organization in the event of an outage.

Reputation Damage

Organizations that experience a significant outage as a result of a ransomware incident will inevitably incur some reputational damage. Typically reputational risk has not been transferrable. For example, if a restaurant company experiences a credit card breach, the customer will still hold the restaurant accountable, even if the restaurant has outsourced its credit card processing to a third party. Today we are seeing insurance companies provide reputational loss coverage that covers lost profit due to reputational damage caused by Cyber incidents.

Data Restoration

Restoring data can be a time-consuming and costly effort. Depending on the number of systems impacted, organizations may be faced with the daunting task of restoring or rebuilding thousands of systems from scratch. For example, following the NotPetya attack in June 2017, it took Maersk 10 days to restore 4,000 servers and 45,000 laptops, at a cost of an estimated $300M. Full restoration took much longer, with reports of staffers working around the clock for two months to restore Maersk's application configurations. Merck and FedEx also made their restoration costs public, with Merck's totaling a staggering $870M, while FedEx's cost $400M. Overall, global costs to restore operations following NotPetya are estimated to be upwards of $10B.

Equipment Damage/Bricking

While distributing ransomware is typically a revenue generating activity for cyber criminals, other forms of malware are designed with a purely destructive purpose, sometimes rendering infected equipment permanently unusable. These types of malware typically impact devices' storage and processing functions. Many times equipment is damaged beyond repair, and when it can be repaired, it requires painstakingly slow and technical remedial work that requires specialized on-site technicians. Oftentimes, it is simply more cost- and time-effective to replace damaged devices. For many organizations, the costs and efforts to replace a sizeable segment of their IT network would be staggering.

Key trends and best practices to mitigate risks

Considering the constantly evolving cyber threat landscape, the following sections explore predictions for ransomware and share best practices for mitigating ransomware risks.

Future trends

There are no indications that ransomware campaigns will become any less relevant in the future. The rise of Ransomware-as-a-Service platforms mean that it has never been easier to distribute malware, regardless of a threat actor's technical abilities and knowhow. Ransomware attacks are projected to cost upwards of $20B in 2021, an almost 100% increase over 2019's projections. Enterprise infections are expected to continue rising as well, with much more targeted campaigns netting cyber criminals a larger profit margin. With the proliferation of interconnected devices and cloud computing, we can expect future ransomware attacks to increasingly target IoT devices and cloud-based platforms and services. Mobile devices will likely be increasingly targeted as well, with a 33% increase in mobile device ransomware infections in 2018 alone. As cyber criminals keep innovating in their tactics, techniques, and procedures (TTPs), organizations and security teams will be hard-pressed to keep up the pace and adapt accordingly. Without an end to ransomware in sight, it is vital to have a well-designed plan to address the threat, as we explore in the next section.

Dealing with ransomware: defense in depth

A comprehensive defense against ransomware requires layered controls to prevent infections, detect them quickly when they occur, and to respond and recover from them efficiently. In the following sections we describe some of the most common controls used to mitigate ransomware risks, organized by the familiar NIST Cybersecurity Framework functions.

Identify

Many businesses struggle to get their arms around the data and underlying infrastructure that support their business-critical processes. It is essential for organizations to define a risk assessment methodology to help identify their critical business operations and to continuously track the risks that could impact them. By doing so, they will have a much better sense of what critical data they hold, where the data resides, and the risks that threaten the confidentiality, integrity, and availability of it. Having this visibility allows organizations to effectively plan investments that protect against cyber threats like ransomware.

Protect

Many businesses built their security defenses and backup solutions well before the ransomware threat materialized. Some built expensive real-time replication infrastructure to address data loss risks, but this solution doesn't help recover from a ransomware attack since infected data is automatically replicated to another site, affecting data in both sites. Instead, it is vital to perform traditional backups and store them offline so that they are inaccessible to ransomware and hackers. There have been instances in targeted attacks where hackers were able to find backups and encrypt them before launching a ransomware attack, rendering their last defense unusable. Therefore, it is important to verify that backups are properly secured and segregated so that they retain their integrity and can be used to recover from a ransomware incident. The effectiveness of these controls should be verified via penetration testing to ensure the backup solution is properly protected by segregation and access controls.

Backup solutions are not perfect. Backups need to be tested to have confidence that they will be viable if needed to restore from a ransomware attack. Many clients tell us that they test their backups regularly when they are asked to restore files accidentally deleted by employees. While this may test a small part of the backup solution, there are other, more complex data sources that need to be tested too, like databases. Also commonly overlooked is the ability to recover applications. In order to test that data, applications, and operating systems can be restored following a significant ransomware incident, organizations should perform a "bare metal" restore by rebuilding systems from scratch with blank storage.

Threat actors usually exploit the weakest link in any organization's security, which is typically the human element, and most ransomware incidents are a result of social engineering tactics or phishing emails. As such, a comprehensive security awareness and training program is the most effective safeguard against ransomware. Furthermore, periodic anti-social engineering and anti-phishing campaigns should be conducted to test the effectiveness of the training program and to identify individuals requiring additional training.

Additionally, technological controls should be implemented to protect against ransomware. Some of the most common are listed below.

- **Email security solutions** – The best email security solutions are those that block malicious emails before they reach the inbox. Such solutions help block emails from known threat actors and provide a layer of protection for emails that contain malicious content, such as attachments containing ransomware or links to known malicious sites. Since malicious emails are the most common infection vector for ransomware, email security solutions are crucial technology to help prevent ransomware reaching your environment.
- **End-point malware protection** – Sometimes malicious emails make their way past initial defense mechanisms, like an email security solution. Today, the best malware protection uses both signature- and behavior-based detection mechanisms to identify and stop malware infections, like ransomware. The newest technologies leverage machine learning to protect against ransomware infections.
- **Intrusion Prevention Systems (IPS)** – If all else fails, an IPS should help to limit inbound and outbound connections required by ransomware and limit its spread if an infection has already taken place.

Detect
Initial ransomware infection is usually easy to detect when it affects a computer since it announces itself by making the computer inoperable and displaying a message that it has been infected. Most ransomware will try to encrypt everything that is accessible to it, both locally and on the network, which usually affects shared drives and other networked storage. Monitoring for unusual changes of this scale will help to detect ransomware infections quickly. A file integrity monitoring (FIM) solution could be used to alert security teams of such activity. Another indicator of compromise is unusually large incremental backups, indicating that a significant amount of data has changed since the last full backup.

Integrating the above information into a 24x7x365 Security Operations Center (SOC) provides security teams with around-the-clock, real-time detection and monitoring capabilities. This enables a timelier response and should help security teams contain a ransomware attack much faster, reducing the overall impact. Such SOC operations do require significant investments in technology, processes, and people. It is not uncommon for small- and medium-sized businesses, as well as larger organizations, to outsource SOC services to a dedicated third-party managed security services provider (MSSP). By outsourcing this function, organizations benefit from a dedicated team of experts that are carefully sourced, trained, and managed, and that have extensive experience that would be very difficult to obtain otherwise. MSSPs also benefit from the information and lessons they learn from their many other clients.

Respond
One of the most significant factors in the cost of a cybersecurity incident is the amount of time it takes to respond and recover from the incident. IT teams need to work quickly once an infection has been detected, which is why preparation is vital for an effective response that includes:

- A well-defined incident response plan,
- A specific playbook for ransomware response, and
- A tabletop exercise or something even more realistic, like simulating a real infection in a controlled non-production environment, to test and improve response procedures.

It is not uncommon for small- and medium-sized businesses, as well as larger organizations, to outsource Security Operations Center (SOC) services to a dedicated third-party managed security services provider (MSSP).

Business leadership should be prepared to answer some tough questions following a ransomware infection, such as:

1. **Has any regulated data been breached (has it left your network)? Do you have the capability to know if it has been breached?**
   Having the right technology in place and configured correctly is critical so that ransomware attacks are detected timely, and so that the organization understands the extent of the incident. Knowing what data has been impacted will govern the subsequent response; regulated data may require notification to regulators and clients within a specific timeframe. Failure to do so may be a costly omission and damage an organization's reputation even further. On the other hand, if the extent of the breach cannot be determined due to a lack of good historical data, an organization may have to disclose more than it normally would have if there had been better certainty regarding the affected data.

2. **Is the ransomware attack a Red Herring?**
   Frequently, cyber criminals use ransomware as a smokescreen. While a victim's IT and Security teams are scrambling to deal with the ransomware incident, the threat actor may be exfiltrating data from the network undetected and unopposed, taking advantage of the chaos of the response. While this is obviously not the case for every ransomware incident, the potential scenario and appropriate checks should be addressed during incident response planning and preparation.

3. **Are you required to publicize the breach? If not, would you do it anyway?**
   Requirements to notify regulators, government entities, or clients may be required depending on the type of data breached and whether an organization falls under the scope of a particular data privacy regulation. However, organizations may elect to disclose a data breach voluntarily without any obligation to do so as a way of managing reputational risk and fallout. In many cases, data breaches are leaked and are publicized by employees or the threat actors themselves. Organizations may want to get ahead of the curve and incorporate appropriate internal and external communication plans into their incident response plans to demonstrate proactivity and transparency in an attempt to maintain or regain consumer trust.

4. **How would you know what's been encrypted by the ransomware?**
   Ransomware is not a subtle type of malware; the purpose of the malware is to very prominently notify you that your data has been encrypted and to solicit payment from you, in return allowing you to restore operations. However, self-replicating ransomware may spread to systems that are not user-facing, encrypting data without any obvious signs. Oftentimes in such cases, the first indicators of compromise are operational failures for unknown reasons as the encrypted data becomes unusable by the systems that are processing it. By investigating the operational failure, teams eventually discover the root cause, which could be ransomware. The time spent investigating the root cause may allow for the ransomware to spread even further, and as such, knowing the extent of a ransomware infection in real-time is vital to mitigate the ransomware's proliferation in the environment. File integrity monitoring solutions are exceptionally useful for such use cases, as they flag and alert on any modification (such as encryption) to critical data and files in real-time. This early detection may allow your teams to get a handle on the situation more quickly, helping mitigate the impact of a ransomware attack.

5. **How would you contain the incident and stop it from spreading?**
   - Ransomware containment requires a strong understanding of the network, which should be well documented and quickly accessible. For example, the IT team should know how they would update switch, router, and firewall configurations to slow or block the spread of the infection. These configurations can be thousands of lines long, so understanding them in advance and practicing how they'd be updated during an incident is critical.

6. **Will you pay the ransom?**
   - One of the most debated and difficult questions to answer following a ransomware infection is whether to pay the ransom or attempt to contain and recover from the infection. While it is easy to take ideological positions, such as never negotiate with extortionists, reality can be a grey area. Frequently paying the ransom may be less costly than the overall recovery effort, and operations may resume faster, making this option a tempting one for many organizations. Other organizations may choose to recover operations using their own methods, disregarding the ransom request for ideological reasons or because they believe they are sufficiently prepared to quickly recover operations at an acceptable cost. Ultimately, there is no right or wrong course of action. It is a decision that business leaders need to take knowing their organization's capability to recover and considering their risk tolerance.

Recover

The most reliable way to recover from a ransomware attack is to restore systems and files from unaffected backups. As such, implementing the right backup strategy is essential. While several variations of the strategy exist, a 3-2-1 strategy is considered the benchmark for an effective backup strategy, which entails the following:

- Having 3 copies of your data at all times (1 production copy, and 2 additional backups),
- Having the 2 additional backups on different storage medias, and
- Having 1 of the backups offsite and disconnected from the network (offline).

Implementing such a strategy ensures that multiple copies of the data are available on different media and in different locations, eliminating any single points of failure. This strategy also ensures that a site-wide failure would not compromise all backup data. Additionally, some ransomware strains have been known to initially target any network connected backup locations and associated backups, crippling a victim's ability to recover from an attack. Ensuring that at least one copy of backup data is disconnected from the network minimizes the risk that this backup data will also be compromised during an attack. Backups for critical systems and applications should be performed regularly using enterprise-grade solutions to ensure their integrity. Backups should be versioned and archived for an appropriate amount of time so that point-in-time recovery options are available. This means that even if the latest backups are corrupted, recovery from earlier, uncorrupted versions might still be possible.

Finally, the simple act of performing backups is not enough; backups should be tested to ensure that data and any dependencies, such as applications and operating systems, can be restored efficiently.

Conclusion

With the rise of Ransomware-as-a-Service platforms, distributing ransomware has never been easier. Ransomware is here to stay, and the costs associated with ransomware attacks are expected to rise upwards of an estimated $20B in 2021, which is a staggering 6,153% increase from 6 years prior in 2015 when the cost was estimated to be $325M. As recent examples have shown, ransomware attacks can wreak havoc on organizations and their operations, and in some cases, require months to fully recover, resulting in significant financial and reputational damage. Basic cyber hygiene across the enterprise is no longer adequate; organizations should be well-prepared to face cyber threats like ransomware. A comprehensively robust cyber posture requires a defense-in-depth strategy, with a layered approach to security. Protective technologies and controls are needed to prevent security incidents. Detective and monitoring controls are essential to detect incidents early and trigger a timely response. Formalized, tested, and continuously improved incident response planning and preparation is key to ensure a coordinated, orderly, and efficient response to incidents that comply with any applicable regulatory requirements. Finally, business recovery planning and periodic testing are required to ensure that recovery processes are streamlined and work as they should when it really matters. Cyber insurance can help as it provides many resources designed to help prepare for and mitigate incidents.

As the financial impacts of cyberattacks, and especially ransomware attacks, continue to rise to record levels, having the right Cyber insurance coverage for your organization is equally crucial, as it can effectively mean the difference between getting back to operations quickly or having a financially crippling setback for your organization.

To learn more, contact your AXA XL Cyber underwriter.

S-RM is a global consultancy that delivers breach response, ethical hacking, and cyber risk and governance services.

5764_06/2019