Ransomware Readiness & Recovery Strategies

How it works. How to Prepare. How to Respond.

(c) 2024 Advanced Logic Industries, Inc.
(800) 283-2648
hello@ali-inc.com

The Cost Potential in Ransomware

Today, ransomware is a business – yes, business. Driven mostly through ransomware-as-a-service platforms run by organized crime gangs, it is the fastest growing threat to business continuity today. A single ransomware attack campaign can net the criminals millions of dollars, in return for very little risk, expenditure or chances of being caught.

Ransomware by the numbers provided by the FBI:
Annual Revenue: $1 Billion+
Infections: 4000+ daily

Ransomware: Today's Threat Reality

Ransomware now impacts organizations of every size, geography, and industry. Some data-centric industries, or those with very valuable data are particularly targeted; but don't think it won't happen to you. It has become the greatest threat to most organizations' operations. So take comfort that you are not the only one facing this menace. Most organizations are struggling to keep up with the shifting threat vectors and non-stop efforts of cybercriminals. It can feel like a game of "whack-a-mole". Once one threat is addressed, another more sophisticated one shows up.

Ransomware now impacts organizations of every size, geography, and industry. Some data-centric industries, or those with very valuable data are particularly targeted; but don't think it won't happen to you. It has become the greatest threat to most organizations' operations. So take comfort that you are not the only one facing this menace. Most organizations are struggling to keep up with the shifting threat vectors and non-stop efforts of cybercriminals. It can feel like a game of "whack-a-mole". Once one threat is addressed, another more sophisticated one shows up.

Today, organizations are having to take a more holistic approach to their data security to protect and prepare themselves. Unfortunately, there is no one-stop security solution. The days of a firewall and antivirus software combination providing adequate coverage are gone. Security software vendors and cyber criminals are racing to out-innovate each other. The hackers are proving themselves to be formidable adversaries.

How Ransomware Works

Ransomware needs a means of entry, some method of delivery, and an ability to execute. Each is a carefully planned component of a ransomware attack.

Phase 1: Hide in Plain Sight.

Like most malware, ransomware finds its way in either via email or maliciously coded websites. The code used at this point is a "trojan" - like the original Trojan horse. Like a wolf in sheep's clothing, it looks credible to end user and applications alike. There's typically nothing about the delivery method that raises suspicion. It looks valid. Even the operating system and virus scanner sees it as a valid type of code that is not out of place.

Phase 2: Just One Click.

Once the trojan escorts the ransomware payload in, its job is complete. There may be many trojans sent to an organization. They are carefully crafted to maximize the chance that someone will click. All it takes is one click to activate the ransomware across a network. Like an army of ninjas, the ransomware code spreads across a network. The faster it moves, the more data it can ransom.

Phase 3: Game Over.

Ransomware accelerates its viral behavior via software macros. Macros are a script of linked activities that enable one to automate a series of activities. When used in installation files, Word and Excel, macros can be very helpful. When used by ransomware, they spread chaos fast to take control of systems and data. Other kinds of otherwise normal code used in Java, Flash, web browsers, and browser plugins can also be exploited. Once the ransomware payload is delivered, your machines will stop working, all data is now inaccessible. All you will see is the ransom demand on screen with instructions on how much and how to pay. Payment is via bitcoin to preserve anonymity of the cyber criminal. You can pay and hope you get your data or, or if you are prepared, you can take control and respond.

(c) 2024 Advanced Logic Industries hello@ali-inc.com (800) 283-2648

Preparing for Ransomware

Assuming it's a when, and not an if, ransomware will strike; it's critical to prepare. Your situation will vary, but best practices include:

Patch Everything, Patch Often.

The average time to develop a vulnerability exploit is just 30 days. Ransomware attacks are leveraging vulnerabilities that are often years old. That means patches exist to plug the vulnerability, but they only work when installed. It's evident that patch management is an issue for organizations of all sizes.

Implement Multi-Factor Authentication

Multi-factor authentication is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence. Implementing this strategy and ensuring consistent usage can cut Ransomware success by over 80%.

Identify Key Assets & Mission Critical Systems

Take the time to locate your critical data. Where exactly is it located. Who is responsible for it? How is it protected? What are the minimum processes and systems necessary to continue operation through a crisis? This is often a patchwork of systems and data that may not even reside within your organization's facilities. Know all you can about your data, including key stakeholders. They, more than anyone, will know the priorities.

Deploy a Multi-Layered Security Strategy

Today, a backup is always part of the ransomer's attack - if they can gain access. So while a backup is important to recover from day to day events, it's important to think more comprehensively about your network security. Securing the perimeter is also just the first step. Now, you need to be looking at securing your data as if you were a criminal. Threats come from many sources including employees, unsecured databases, unsecured mobile devices and more. And, because hackers know your business hours, it's increasingly important to make sure there is monitoring and cyber response around the clock. Your team may not be working, but hackers often unleash their worst just as your weekend or holiday is underway. This is no accident.

Our **FLxSecure Services**help you assess your current security state and design strategies to ensure your organization is protected. Additionally, our **FLxStore Data Protection** service provides an ideal solution for your 3-2-1 backup strategy. Our FLxStoreDR IT Recovery Readiness cloud service provides operational readiness to ensure business continuity.

For critical data, a secure cloud-based archive solution provides even better IT recovery. Archives save your data in real time rather than a single point during the day, so on the day of a breach or outage, the amount of critical data lost prior to that day's backup is significantly reduced. We recommend and implement Donoma OneVault as it is a cloud archiving platform that can manage many different data types at once.

Proactively Monitor for Threats.

There's a wide range of services and tools to help you monitor the security of your IT infrastructure that is no longer neatly contained inside a limited number of office locations. It is critical to understand that IT security is layered and must be adaptable. The "hard candy shell" approach that relied on security only at the perimeter is no longer acceptable

Create a Culture of Security Awareness

The number one threat vector are staff members themselves. While most would never want to cause harm to their employer, they all need to be educated and made part of your security strategy. Teach employees about phishing and security challenges, Make sure they are set up with multi-factor authentication when accessing services on your network. Help them recognize threats and ensure they know how to respond in the moment. An educated workforce is a powerful asset in your security plan.

Build & Test Your Emergency Response Plan

If you knew the chances were good that you might experience a fire in your office, you'd make sure you ran fire drills. You post instructions to help people during an emergency and you practice ahead of time. The same is true for a data security emergency. Plan ahead and the stress and very real disruption can be made more manageable when a tested plan is in place.

Unless you Have the Resources, Don't go it Alone

Cyber-Security is a fast changing field of very specialized capabilities. Unless you already have a team of people on staff with this expertise and you are committed to a continual upgrade of systems, tools and training, your best bet is to engage some professional help. Just as you engage lawyers and CPAs to handle specialized areas of expertise for your business, the same is true for Cyber-Security. Our FLxSecure services provide you proactive monitoring and a fully staffed threat response team in the event of a a problem.

Emergency Ransomware Response - Initial Steps

Your ransomware plan can't just contain the steps designed to stop malicious code entry. Your plan must include measures that allow rapid response, involvement of key stakeholders inside and outside your organization a plan for Return to Operations (with timeframes identified in advance) to guide service and data restoration. The goal is to reduce downtime to the bare minimum, and return to normal as quickly as possible.

Some might think it cheaper to simply pay the ransom. That's a terrible idea for at least three reasons:

1. It's not uncommon that organizations never get their data after paying the ransom. The cyber criminals have your money and you can't trace them. There's no customer complaint department when dealing with criminals.
2. If you can recover the data, it may be corrupted and won't decrypt with data integrity maintained. Instead, rely on data recovery from your own tested backups. It provides 100% confidence in your recoverability and return to normal operations.
3. If you rely on decrypted data, you have to find and remove the ransomware code that is still in there! Cyber criminals don't clean up after themselves.

According to a recent survey by Citrix, 36% of organizations are not confident they can eradicate malware after the fact. In our experience, that number is under-stated. We'd put that number well over 66%. This takes a very particular skillset.

1. Identify Your Threat: Source, Vector and Damage

When an attack happens, you need to know what's impacted, where it originated from and what has been impacted as a starting point for your response.

If you have a Cyber Insurance policy, this information will be required before any remediation can start.

In fact some policy holders are dismayed to discover that they insurance companies aren't concerned with getting your business back to business right away. They want to see if there's an grounds for them to not pay because of gross negligence. Only once they have the source and vector will they allow access to systems to begin the recovery process. Proactive deployment of cyber-security monitoring systems and services can significantly reduce this necessary step in the process. Without it, we have seen data restorations that could be completed in days remain offline for weeks.

2. Recover the Server Data.

Ransomware connects from the infected computer to any servers it can reach via existing or cached connections. The end user device is the "snack" on the way to the big prize - servers and application data. An infected end user computer can easily allow ransomware to encrypt files on many servers at once. To be certain data is back in a production state, restoring the affected data set is vital. Because you won't know ahead of time what data may be affected; it's a best practice to back up both end user and system data. We recommend a 3-2-1 data protection strategy with an archive system for critical information.

3. Have a Plan for User Devices.

Whether notebooks, desktops or other computing devices, all harmed by ransomware need to be wiped and reset. This removes any traces of ransomware; then data from your backup will need to be restored. Devices used by key users or functions may need image-level backups to prioritize their return to normal operation. Other users can use a redeployed standard workstation image.

4. Engage Your Emergency Communication Plan.

Much like a fire drill, training everyone how to react in an emergency increases response success. Train your employees and prepare a response plan in advance. During an incident, keep key team members informed according to the plan. This reduces stress, provides transparency and supports a more graceful return to normal.

Next Steps & Additional Resources

IT Security Matters.

Don't go it alone. We're here to help.

Talk to us & see how affordable it can be to engage professional help for significantly less than you think.

Click Here to Schedule with Us