Ransomware: Seven Lessons Learned

HOW TO MAINTAIN A SAFE, SECURE IT INFRASTRUCTURE

FLAGSHIP
NETWORKS

100 Beard Sawmill Rd
Suite 340
Shelton, CT 06484

203.358.0800

FlagshipNetworks.com

THIS YEAR IN RANSOMWARE

Twenty twenty-one has been quite a year for ransomware attacks. Cyber criminals focused their sights on many organizations, using different methodologies such as riding on the supply chains of SolarWinds and Kaseya, to hitting large and small organizations including Colonial Gas, JBS Foods, schools and towns. Ransomware attacks are up 151% this year, according to Sonic Walls' *Midyear Threat Report*. The trends suggest that the attacks are not likely to stop.

The impacts are significant, including the loss of revenue, reputational damage, and unplanned workforce reductions, as well as the potential for unrecoverable data loss. According to a recent Cybereason report, "Ransomware: The True Cost to Business," global ransomware damages are projected to reach $20 billion this year. The average payout per organization rose from $6,000 in 2018 to $178,000 in 2020.

> *80% of organizations that paid a ransom were hit by a second attack within weeks of the first attack – almost half were hit by the same threat group.*
>
> Cybereason, Ransomware: The True Cost to Business

The one constant has been that cybercriminals change their tactics. They have made direct attacks to large companies that are able to pay sizeable ransoms, as well as attacked smaller organizations through so-called "supply chain" tactics by which they piggyback on a technology provider to gain access to the IT infrastructure. Cybercriminals are learning from each experience and creatively determining their next approach.

Organizations must learn from these experiences to protect their business. The following are seven lessons that we would like to share with our clients. Some of the lessons relate to technology, but many are simply the best practices that will help keep your business safe and sustain operations during and after a cyberattack.

1 TRAIN EMPLOYEES ON CYBER SAFETY

Ben Franklin coined the phrase, “An ounce of prevention is worth a pound of cure.” This axiom absolutely applies to ransomware and cybersecurity in general.

> *More than 99% of cyberattacks require human interaction to succeed.*
>
> ProofPoint *Human Factor 2019 Report*

Your exposure to a cyberattack is significantly reduced if employees know how to detect and react to suspicious emails, the importance of more secure password protection strategies and proper use of your organization’s workstations, laptops and any device connected to a network. Even practices that may appear innocent like having passwords on sticky notes on the monitor may be exactly the opening a cybercriminal needs to get into your network.

This is the simplest lesson to implement, and it helps to reduce human errors that give cybercriminals the opening they need to get into your network. During security audits we find that employees have put passwords on sticky notes attached to their monitors, left server rooms unlocked, or allowed staff to connect to the network with unauthorized devices. Not all cybercriminals live in foreign countries or have ties to crime networks like REvil, who was behind the Kaseya Independence Day attack. Some may arise from employees within the company.

Work with your Managed Service Provider (MSP), technology providers or cyber insurance carriers to find sources of good training materials and if necessary, develop customized training for your organization. Key areas to cover are how employees can identify phishing and other cyber-attacks, safe web browsing, data security practices, as well as informing employees of your organization’s password, device management and incident response policies.

2 CREATE AN INCIDENT RESPONSE PLAN

How should employees act when there is a cyberattack? An Incident Response Plan is a guide for what to do, who to call and what to communicate. Companies with a solid Incident Response Plan fare much better than those without. They can help employees stop an attack early and leave the next steps to the professionals, who can determine the cause and the strategy for remediation.

What to do? The first and simplest thing to tell employees is that if they detect an attack, turn off their workstation and disconnect it from the network. That will prevent the attack from moving laterally across systems within your IT environment. Time is of the essence. Plus, it may save any evidence of the attack on the workstation for the insurance and/or forensic firm.

Who to call? The first call should be to the office manager or internal IT team. Before an employee talks to anyone outside the organization, you should engage the company’s single point of contact, who will coordinate all communications, both internally and externally. That person should have a short list of senior people (e.g., CEO, Principals, owners, etc.) who need to be informed immediately.

Who to call next? Call your MSP or the IT services provider who may be connected to the event. They may be seeing the attack at same time, and if not, they need to be alerted that your organization may be threatened. Never sugar coat the situation when communicating with service providers. At the outset, it is difficult to detect how widespread an attack may be. Are you the only affected party? Is this part of the broader set of incidents? Either way, the service provider will be able to guide you on your next steps and how to get your IT environment operational ASAP. They can examine each workstation and server that appears to be impacted, test them 1-by-1, and install tools to fix the issue.

If you know that you might incur damages, whether due to the loss of data or request for a ransom payment, you must communicate with your cyber insurance agency early in this process. They need to be apprised of the situation and may want to contact (or recommend to you) a forensic consultant to determine the cause and damage of the incident.

Whether a broader set of employees or the whole organization are eventually informed is highly dependent on the nature of the attack. Many banks, public institutions, professional offices, hospitals, and other organizations may want to limit knowledge of the attack to affected customers for reputation purposes.

Understand your vendors' Responsible Disclosure Process. Many MSPs and technology vendors have a Responsible Disclosure Process, which is their internal plan for how to communicate with clients in a timely way about cyberattacks. This is not necessarily a detailed plan, but their runbook for how to connect with clients in the event of an emergency. Ask your MSP and IT providers for their policy so that you have a complete picture of what information you can build into your plan.

Document your Incident Response Plan. Your plan should be documented and stored in two places, one outside your environment (e.g., DropBox, Box, etc.) and one available in paper form. It should include multiple forms of communication, such as personal emails, phone numbers, web conferencing links, etc. Make sure that your MSP has your emergency contacts and updated Incident Response Plan, so they know how to best support you if an attack occurs.

3 DEVELOP A BUSINESS CONTINUITY PLAN

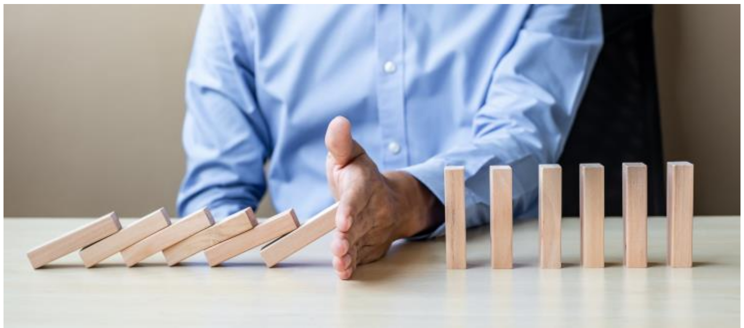
A Business Continuity Plan (BCP) is a complement to your Incident Response Plan. It addresses, "How do we conduct business manually when systems are compromised or down?" And it applies to anything that causes a disruption in business, from power outages to extreme weather events to cyberattacks.

If your business is a hotel or private club, how do you handle reservations or process receipts? If you are a hospital, how to accept patients or track procedures? If you run a school, how do you continue instruction or communicate with parents? Do not assume that the staff knows how to go back to the old way of doing things. Document key processes in a "run book," and do drills on a regular basis, at least as frequently as required to keep the staff informed.

The BCP can keep you from panicking during a cyberattack. When you panic, bad decisions are made. Have your back-up plan in place, so that business can continue while you work on solutions.

4 ESTABLISH A DATA PROTECTION PLAN

Your data is the most important thing to protect. Many ransomware attacks focus on removing or locking data to hold for ransom. The *Cybereason Report* states that only 51% of organizations hit by a ransomware attack were able to regain access to their data without some or all the data being corrupted.



Back up data to a location that is "air gapped" (i.e., disconnected) from your network so cybercriminals cannot access it. This method will lower your exposure to paying the ransom if data is locked or stolen, as it can be restored after an incident is resolved. You should back up everything, including emails, transactions, business applications – not just what is stored in company databases – to multiple locations (i.e., both on-site and off-site). The locations should be monitored, as well, to ensure that a cybercriminal has not planted code that they can activate later.

Your retention policy, i.e., the length of time you need to maintain back-ups, depends on the dataset. For example, financial records are typically kept for seven years. An individual employee's laptop files may need only be kept for a brief period if they run weekly back-ups. You must prioritize data sets that are critical for running the business if attacked and determine the frequency to run each back-up.

INSTITUTE & TEST YOUR DISASTER RECOVERY PLAN

5

Now that you have your data backed up, it’s time to test how to restore it so that your organization can get back to business as usual. You may need to do multiple rollbacks depending on what’s affected, e.g., your workstations, servers, and your data file-by-file.

We recommend conducting disaster recovery tests and audits on a regular basis, the frequency depending on the size and complexity of your environment – testing could be done annually, semi-annually, or even monthly. Some organizations do not believe there is an immediate benefit to this step, because it requires testing a capability that they believe they already have. They feel secure. However, real security is proving that you can get the business back up and running quickly after a cyberattack.

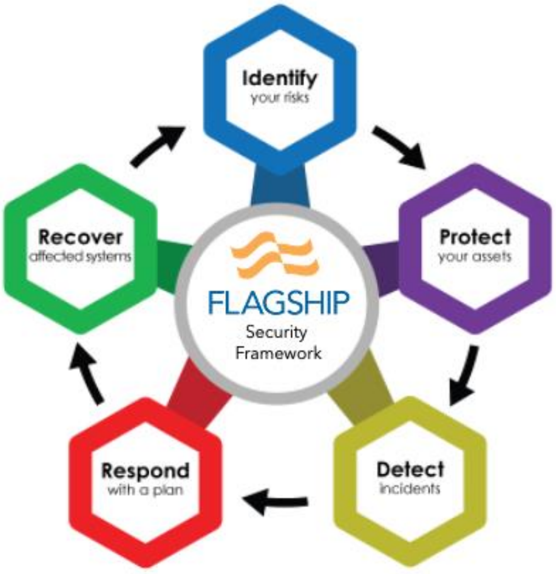
IMPLEMENT A SECURITY STACK THAT FITS YOUR ORGANIZATION

6

There is no one security tool or set of tools that protects every organization. You must work with your MSP or security vendors to determine “the stack” of technology that best protects your organization. Clients who regularly review and implement security recommendations have either avoided cyberattacks or once breached get back up and running quickly with minimal impact.

Most organizations are employing the basic tools, such as a firewall, anti-virus protection on workstations and servers, as well as back-up and recovery for those systems. It has become clear, however, that basic tools do not provide enough protection anymore. Simply getting the latest version of these tools may not do the trick either, despite vendor claims. Organizations need comprehensive visibility across the environment, and the ability to analyze indicators of network behavior or compromise. Behavior provides clues about what is happening now, or what may happen soon, as opposed to a compromise which focuses on reacting once a malicious action has occurred.

The Flagship Security Framework is an outcome-driven methodology which determines the technology and processes that will help clients protect their organization. It represents five core functions in a security lifecycle that enables organizations to **Identify**, **Protect**, **Detect**, **Respond** and **Recover** in the event of a cyberattack. By applying this lifecycle to the main components of an IT environment – Users, Endpoints, Infrastructure, and Network – you can determine the best technologies and processes that will keep you safe.



In addition to infrastructure and software systems, we recommend adopting policies that maintain the health of your protection, such as:

- Do you have a lock-out policy to prevent users from logging in after several tries?
- Do you have multi-factor authentication (MFA) to ensure all logins are from your staff? The US Cybersecurity Infrastructure & Security Agency (CISA) recommends that all organizations implement multi-factor authentication on every single account that is under their control.
- Do you employ a “zero-trust” policy so that devices that connect to the network are not trusted by default?
- Have you adopted the principle of least privilege on key network resources to limit access to only individuals who need it?
- Do you have a safe location or system to store key documents (e.g., Incident Response and Business Continuity Plans) for access when all other systems are down?

Flagship can help implement these critical policies and related security features in all your cloud and edge services.

7 CONDUCT A SECURITY AUDIT

Your first step to mitigate the risks of a cyberattack may be to conduct a cybersecurity audit. A comprehensive audit is a review of your entire IT environment, including user accounts, workstations and servers, system patch history, business applications, and back-up data storage. In addition, you must review key process runbooks, such as their Incidence Response and Business Continuity Plans.

Each system should be assessed to detect issues based on industry-wide best practices for network health, performance, and security. An audit also provides an inventory of discovered assets, including inactive systems, and their operating systems.

At Flagship, our audits deliver a risk score that reflects both the number and severity of detected issues (0 represents no issues). The overall score reflects issues with the highest-level risks, not simply an average of the individual system scores. An overall issue score of zero is unlikely given that specific circumstances will offer some risks.

A comprehensive security audit enables clients to understand their risk exposure and provides a guidebook for how to improve their defenses. Audit recommendations for each system and the overall environment include:

- Technologies to update or acquire (e.g., missing security patches, acquire dark web monitoring software, end-point detection systems)
- Process changes (e.g., passwords should have expiration dates, need to test disaster recovery runbook, etc.)
- Physical adjustments (e.g., inactive computers still have network access, staff have passwords on post-it notes, server rooms are not secured, etc.).

Shortly before the Independence Day REvil ransomware attack, we conducted an audit for a managed service client to ensure that all their systems and processes were up to date. That simple action enabled them to quickly respond to the attack and get back to work ASAP with minimal disruption.

UNDERSTAND YOUR CYBER RESPONSIBILITY

Whether you have a managed service provider, or your own IT team manage your infrastructure, protection from cyber criminals is a shared responsibility between you, your service providers and technology vendors.

The Independence Day REvil attack was a supply chain attack directed at Kaseya's Virtual System Administrator (VSP) technology to reach organizations through their managed service providers. It impacted thousands of organizations. Other security technology vendors jumped in to provide their own assistance to customers, despite not being the target for the attack. The size and complexity of this attack left many organizations with their heads spinning.

Make sure that you have the right personnel on the job, whether on staff or through their MSP. The right skills help to ensure that ransomware attacks are either blocked outright with effective security solutions and controls, or at a minimum are detected and mitigated early before it escalates to the point where it damages the business.

Work with your MSP or key technology service providers to ensure that you have done everything in your power to prepare. If you walk through the seven lessons above and put the proper plans and procedures in place, you will significantly mitigate your organization's risk from ransomware and other cyberattacks.

Your trusted partner for technology and services

Flagship Networks is a proven, trusted Managed and Professional IT Services organization that operates as an integrated arm of your businesses — understanding, predicting, and solving your business IT challenges.

FLAGSHIP
NETWORKS

100 Beard Sawmill Rd
Suite 340
Shelton, CT 06484

203.538.0800

FlagshipNetworks.com

© Flagship Networks. IT Sentinel is a trademark of Flagship Networks, Inc.