Expecting the Unexpected: Tips for Effectively Mitigating Ransomware Attacks in 2021

Cybercriminals continually innovate to thwart security protocols, but organizations can take steps to prevent and mitigate ransomware attacks.

JUNE 2021

by Luke Tenery and Ross Rustici

Luke Tenery
Partner, StoneTurn
ltenery@stoneturn.com
+1 312 775 1210

Ross M. Rustici
Managing Director, StoneTurn
rrustici@stoneturn.com
+1 617 570 3716

2020 was a watershed year for ransomware attacks, and 2021 is showing more complex and destructive extortion schemes targeting energy and critical infrastructure, schools, hospitals, law firms, government agencies, and corporations. With damages from cybercrime expected to soar this year, threat actors are continuing to exploit businesses and individuals distracted by the pandemic.

The good news is that, even as cybercriminals continually innovate to thwart evolving security protocols, organizations can follow a proven playbook to help prevent and mitigate ransomware attacks.

Prepare for Seemingly Improbable Scenarios

Long before a ransomware attack, much can be done to prepare from a technical perspective. Have a detailed current data map so that you know exactly what is on any affected system. Identify technical backups and ensure they are ready for rapid deployment to minimize any gaps from data loss. Further, develop well-documented addendums to your incident response and data recovery plans that are specific to cyber and ransomware issues.

Many organizations think they are prepared for data recovery after an attack by testing and confirming they have good backups in place. However, savvy ransomware attackers are now compromising organizations' backups by encrypting or deleting them altogether. Further, it may be difficult to leverage backups quickly enough for the broad, sweeping effects of a widespread outage caused by ransomware. You should consider these contingencies in planning.

Tabletop exercises and threat-modeled scenarios — which simulate the tradeoffs and dynamic choices the incident response team must make in a crisis — are extremely helpful to develop these addendums. These exercises should be informed by the current threat landscape and the likeliest risk scenarios facing your business. Focus on issues that will impact the entire organization, and bring in stakeholders from across the company to understand how threat identification, remediation, and reporting affect the entire enterprise, not just the security organization.

Understanding and agreeing upon response options for items such as the limits of cyber-insurance policies, international reporting requirements, data retention policies, and go/no-go protocols for enterprisewide mitigation procedures (such as global password resets or customer communication) are the difference between a minor service interruption and front-page news in a ransomware incident. Waiting to address and debate these issues until you are in the middle of a response action leads to suboptimal outcomes and extended recovery time.

Last, but certainly not least, assume the worst: Any single control can be bypassed or fail. Resiliency plans should focus on what layers of defenses can be put in place to proactively mitigate this possible scenario. Network segregation, a zero-trust policy for third-party software (a lesson learned from SolarWinds), and advanced detection and response controls can help limit an organization's risk exposure should any line of defense fail. Advanced detection and response should also include advanced malware detection and threat hunting.

Many organizations incorrectly assume that ransomware's impact is the immediate effect of the cyberattack. Most often, attackers stage other effects, including compromising other security weaknesses. Advanced controls shorten the time to detection and the attacker's time to stage attacks, increasing the chances to catch illicit activities before ransomware is deployed. Advanced detection and response practices can minimize the impact of exposures that ransomware attack groups intend to leverage for an increased likelihood of payment.

Proactively Mobilize a Multidisciplinary Team and Strategic Redundancies

Given that cybersecurity is not IT's problem alone, assemble a multidisciplinary team spanning IT, investor relations, communications, legal, marketing, sales, and HR to respond to ransomware attacks and other crises. Ransomware should be treated like any data breach, with a cross-functional team mobilized to follow and implement an established playbook and response plan. To maximize efficiency, incident response team members should meet regularly and clearly document responsibilities and escalation points for various crisis scenarios.

Extortion attempts now include public shaming and customer-data exposure. Further, double-payment requests are on the rise, so the threat remains even after making payment. Therefore, customers, employees, and shareholders cannot be kept in the dark and may even have roles in minimizing ransomware's impact.

Make sure to have another means of trusted communication at the ready in case companywide email is compromised in an attack. This "out of band" communication system is critically important to maintaining normal business operations and providing key constituents with a trusted source of reliable information in a crisis. This platform should be tested and users taught that it is an acceptable alternate communication method.

Document Lessons Learned and Provide Post-Event Assurance

You need a combination of attack detection, data security, and data backup to effectively weather a ransomware attack. The post-event path forward often receives less attention and fewer resources. Unfortunately, hackers are increasingly using automation to attack business networks, spot patterns of defense, and identify vulnerabilities in similar systems, so thorough remediation is key. To avoid enforcement action and irreparable reputation damage, you must be able to demonstrate that appropriate corrective action has been taken. There is also much to learn in the wake of successful and unsuccessful cyberattacks.

As a first step, undertake a thorough investigation to identify the extent of the breach, pinpointing all exposures and the ransomware's navigation throughout the system. If the public is aware of the attack, an independent third party can provide objective assurance that the threat is eradicated. Further, outside experts can also suggest and implement enhancements to internal controls, policies, and procedures to prevent similar future attacks. It is wise to monitor external open source and Dark Web intelligence channels for continued indicators of information exposure. Finally, if reparations are in order, third parties can oversee the required reporting (8-K filing, media release, HIPAA notifications, etc.) and take the lead on restitution processes to enable the recovering organization to focus on resiliency and return to business as usual.

This article originally appeared in **Darkreading, June 2021.** All rights reserved.

About the Authors

Luke Tenery, a Partner with StoneTurn, brings nearly 20 years of experience helping leading organizations mitigate complex cybersecurity, data privacy and data protection risks.

Ross Rustici, a Managing Director with StoneTurn, has over a decade of experience advising governments and global corporations on cybersecurity matters, as well as building security and intelligence programs for clients.

Leaving no stone unturned.

StoneTurn, a global advisory firm, assists companies, their counsel and government agencies on regulatory, risk and compliance issues, investigations and business disputes. We serve our clients from offices across the U.S., U.K. and in Germany, Brazil and South Africa, assisted by a network of senior advisers around the world.

StoneTurn.com

StoneTurn