3 Best Practices to Prepare for a Ransomware Attack

Cyber-attacks remain a top business risk year after year, increasing in frequency, severity, and sophistication. At the top of the cyber-attack list? Ransomware.

As the remote workforce from the pandemic expanded, ransomware attacks increased 148%. Bad actors have discovered a rich environment of unsecured WiFi, vulnerable equipment, and outdated intrusion prevention software. Attacks are not only more frequent, they're swifter — a new remote desktop protocol (RDP) is discovered just 90 seconds after it is opened to the internet.

Ransomware has become an industry, and every organization is a potential target. Attacks now routinely disrupt operations for days or weeks; the average downtime in the fourth quarter of 2020 was 21 days. In addition to downtime and remedial expenses, ransomware demands have skyrocketed, with extortion demands increasingly exceeding $10 million.

More than 70% of attacks now also include data exfiltration, which bad actors use as a coercion tactic to entice companies to pay higher ransom demands. Layer in regulatory and compliance considerations, and you've got a complex issue to navigate.

Companies with poor cyber hygiene can become low-hanging fruit. Cyber-attackers are constantly evolving their tactics and scanning corporate technology environments to identify companies with poor cyber hygiene, such as lax controls or unpatched software. The increase in attack sophistication shows no signs of slowing.

Organizations that take a robust approach to ransomware preparation can increase their odds of avoiding an attack, recover more quickly, and minimize the impact of an attack. It's critical for organizations to be prepared well in advance of a potential incident.

The bottom line: Planning is everything. Read on for three of the best practices that an organization can adopt.

1 Best Practice: Develop and Test Incident Response Plans with Ransomware in Mind

PREPARING FOR A POTENTIAL ATTACK

Your organization should have an effective cyber incident response plan in place that specifically includes ransomware. Unfortunately, many organizations with a plan in place do not update it — or test it — to address new risks. In fact, fewer than 50% of organizations have reviewed or updated their cyber incident response plan in the past year and only 40% planned to invest in cyber incident planning and preparation, according to the 2019 Marsh Microsoft Global Cyber Risk Perception Survey.

Here are some steps you can take immediately to prepare for a potential ransomware attack:

- **Plan and test.** Develop or update your existing incident response plan to include ransomware considerations. Once your incident response plan is in place and accounts for ransomware, it is time to put it to the test. Evaluate your incident response plan with a ransomware tabletop exercise. Practicing a hypothetical ransomware scenario is critical for the quality of a real ransomware response.
- **Develop a decision-making framework.** Use this to help analyze whether you can restore data and systems on your own and whether it makes sense to pay an extortion demand. The framework should include criteria to analyze specific circumstances, including the criticality of impacted data and systems, the length of time your organization can operate without critical data and systems, and the cost and length of time for your organization to restore the impacted data/systems on your own and/or with external support. Engaging external counsel to help develop and review the framework is recommended.
- **Establish ransom payment criteria.** When developing ransom payment criteria, include the amount of the initial extortion demand, the threat actor's track record of negotiating the initial demand downward, the threat actor's history of providing working decryption code upon payment of the ransom, and an estimate of the length of time it will take to restore data and systems using the decryption code.

  Include criteria in the framework to assess circumstances where the threat actor demands payment in exchange for not releasing stolen data to the public. This includes analyzing what data the threat actor actually has via a "proof of life" process and evaluating the potential reputational or other harm that would result from a public data disclosure. We recommend having an external extortion service provider review your payment criteria.
- **Identify extortion service providers in advance.** Some extortion services are available on a standalone basis while others are part of services offered by digital forensics providers; many insurers have vendor panels that include extortion service providers. Extortion services typically include providing threat intelligence, negotiating with threat actors, ensuring compliance with regulations and restrictions such as the Office of Foreign Assets Control (OFAC), procuring cryptocurrency, and conducting payment transactions.
- **Engage legal.** In addition to extortion services providers, know which incident response vendors to engage when an attack hits. This includes a law firm that specializes in cybersecurity and data protection and a digital forensics incident response provider. Many cyber insurance policies cover incident response vendor services, which are frequently subject to prior consent, and many cyber insurers have panel vendor requirements. Ensure legal counsel is involved in and ideally directing ransomware analysis and overall investigation to maximize attorney-client privilege. Legal counsel can also provide guidance on notifying law enforcement of ransomware attacks, a practice that is encouraged by regulatory agencies.
- **Consider regulatory and compliance requirements.** Have a compliance program in place to specifically address the possibility of paying a ransom demand. Organizations should follow OFAC guidance and review their plans with all key stakeholders, including outside counsel and other parties that specialize in ransomware response.
- **Keep your checklist handy.** Maintain ready access to an incident response checklist, including how to engage your cyber insurer and what vendors to engage when. This can enable a more efficient and seamless response.

2 Best Practice: Be Diligent About Cyber Hygiene

The top three ransomware attack vectors are RDP compromise, software vulnerabilities, and email phishing. Improving cyber hygiene can help limit potential exposure to attacks. At a minimum, companies should focus on the following hygiene essentials to mitigate the effects of a ransomware attack:

- **Ensure regular backups and periodic data restoration testing.** Storing backup data offline and offsite in a secure manner can substantially expedite recovery from an attack. Limiting access to privileged users is also important.

A full backup should be completed at least once a week, although more valuable data may need to be backed up more often and incrementally. Businesses should conduct tests to confirm that backed up and restored data will work in a live environment.

- **Segment your networks into smaller sections.** Use firewalls and other means to limit opportunities for attackers. Without gaining privileges, unauthorized users ideally will not extend beyond the originally compromised segment.
- **Limit access.** Require multifactor authentication (MFA) for users accessing critical or sensitive data. Remote access should also require MFA through encrypted VPNs.
- **Update your software.** Patch regularly to maintain the security of applications and operating systems. Address all critical patches immediately.
- **Enhance security awareness.** Cybersecurity awareness training for employees is an important cyber hygiene practice, as employees are the first line of defense against phishing attacks. Employees should be trained to recognize phishing emails and other threats. At the same time, security tools can also prevent phishing emails from reaching an employee's inbox.

3 Best Practice: Understand the Financial Impact of Ransomware and Transfer Residual Risk

Consider ransomware as part of your organization's broader risk management efforts. Take into account your risk tolerance, cybersecurity controls, cyber insurance coverage, broader enterprise risk management programs, and value chain as you review and develop your ransomware plans and prepare for the possibility of an attack.

QUANTIFY YOUR RANSOMWARE EXPOSURE AND STRESS TEST YOUR BALANCE SHEET

Quantifying cyber risk in financial terms allows you to express cyber risk in a language common to all business stakeholders: economics. Equally important, quantification allows organizations to frame cyber in the same terms as other business risks and evaluate risk management investments on the same financial basis.

Ransomware attacks can be devastating from a cost perspective — and the impact of an attack is directly tied to an organization's controls and incident response planning. Consider the cost of your systems being down for 14 business days as you rebuild your network from scratch. Was data stolen? Will you negotiate with the bad actor?

Ransomware attacks can play out in countless ways. It's important to consider the financial impacts they could have on your organization and your balance sheet's ability to cover these costs. Due to the unpredictable severity of such attacks, many look to transfer their risk and turn to cyber insurance.

TRANSFER YOUR RISK

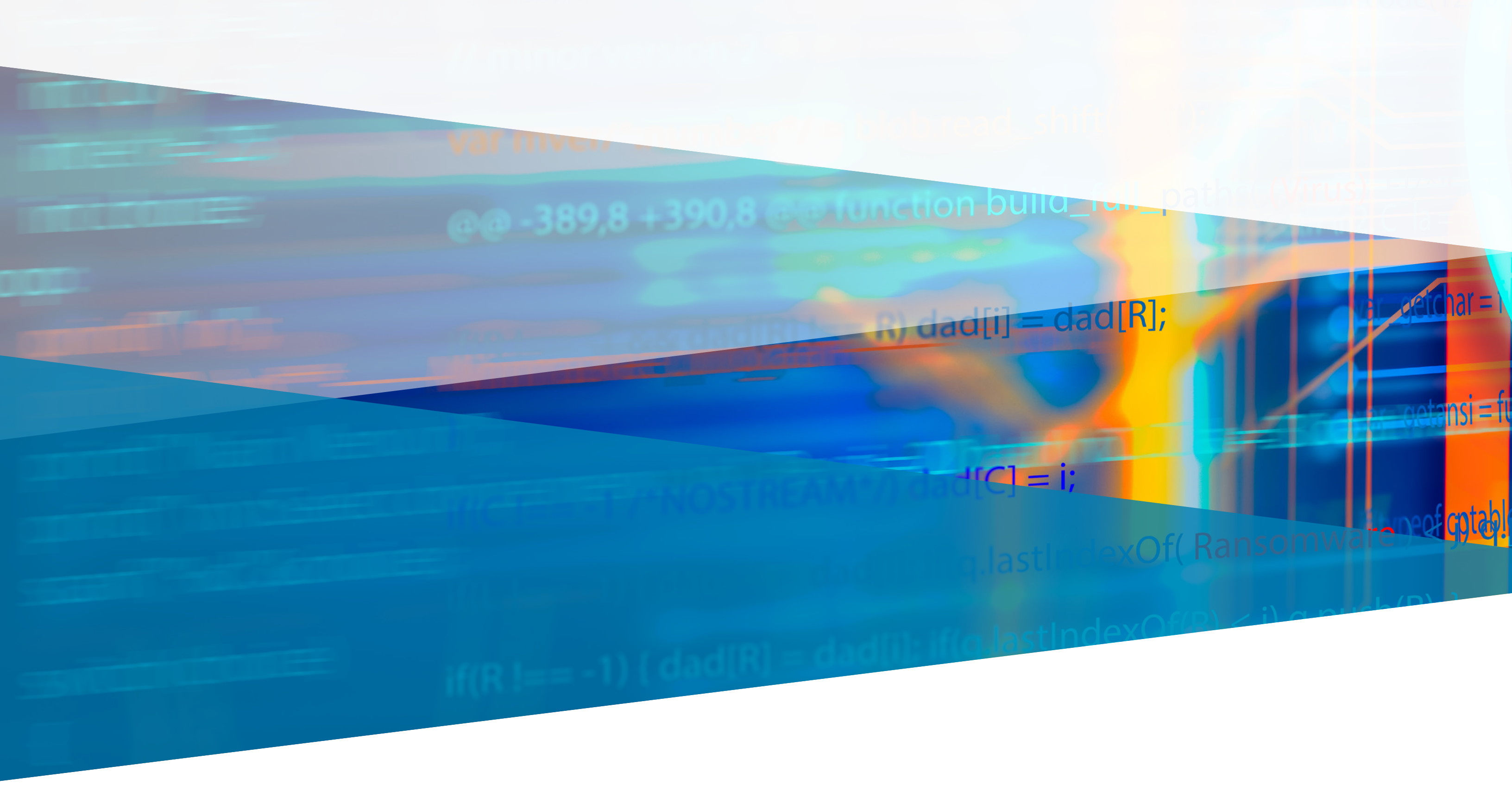
While understanding the financial impact of your ransomware exposure is essential, it's only one piece of a comprehensive cyber risk management strategy. Risk transfer can help protect an organization's balance sheet and provide resources if risk mitigation tactics fail.

Cyber insurance can provide comprehensive coverage for ransomware attacks, including for ransom demands, business downtime, and associated costs. Cyber policies may also provide access to vendors to help with response as well as resources for clients on incident response planning, employee training, legal, forensics, and breach notification services.

PREPARING FOR RANSOMWARE ATTACKS

Ransomware attacks can happen to anyone. Planning can make all the difference.

Have ransomware questions or need help? Click here to learn how Marsh has helped organizations just like yours, all around the world, prepare for ransomware attacks.


@@ -389,8 +390,8 @@ function build_full_path
R) dad[i] = dad[R];
dad[C] = i;
q.lastIndexOf(Ransomware
if(R !== -1) { dad[R] = dad[i]; if(q.lastIndexOf(R) < i) q.push(R) }

For more information and other solutions from Marsh, visit marsh.com, or contact your local Marsh representative.

REID SAWYER
Practice Leader
US Cyber Risk Consulting
Marsh Advisory
+1 630 442 3506
reid.sawyer@marsh.com

SUSAN YOUNG
Managing Director
US & Canada Cyber Practice
Marsh
+1 206 214 3161
susan.young@marsh.com

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.