www.hometownconnections.com
12081 W. Alameda Parkway, # 464
Lakewood, CO 80228
P — 970 682 4217

Hometown Connections

June 2021

3 Best Practices To Prepare For A Ransomware Attack

Including Elements Of A Comprehensive Incident Response Plan

Cyber-attacks remain a top business risk for all utilities and municipalities, increasing in frequency, severity, and sophistication. At the top of the cyber-attack list? Ransomware. The recent attack on the Colonial Pipeline is focusing heavy attention on the threat of ransomware on U.S. energy infrastructure. The bottom line: planning is everything. Learn the three best practices for preparing for a ransomware attack and how to create a detailed incident response plan that prevents paralysis should the worst happen.

As the remote workforce from the pandemic expanded, ransomware attacks increased 148%. Bad actors have discovered a rich environment of unsecured Wi-Fi, vulnerable equipment, and outdated intrusion prevention software.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, with every utility and city as potential targets. 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.

Poor Cyber Hygiene Is Red Flag For Attackers

Community-owned utilities and municipalities with poor cyber hygiene are low-hanging fruit because cyber-attackers are constantly scanning for opportunities such as lax controls or unpatched software. Organizations that follow the three best practices for ransomware preparation can increase their odds of avoiding an attack, recover more quickly, and minimize the impact of an attack.

1 Develop and Test Incident Response Plans with Ransomware in Mind

PREPARE FOR A POTENTIAL ATTACK. Your utility and city should have an effective cyber incident response plan in place that specifically includes ransomware.

- **Plan and test.** Develop or update your existing incident response plan to include ransomware considerations. 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. 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 to assess circumstances where the threat actor demands payment in exchange for not releasing stolen data to the public. 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.

Be Diligent About Cyber Hygiene

The top three ransomware attack vectors are RDP compromise, software vulnerabilities, and email phishing. At a minimum, community-owned utilities and municipalities 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. 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. Limiting access to privileged users is also important.

- **Segment your networks into smaller sections.** Use firewalls and other means to limit opportunities for attackers.

- **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.

- **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.

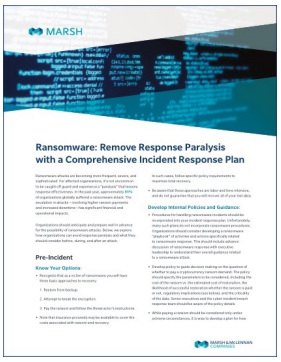
3 Understand Financial Impact of Ransomware & Transfer Risk

Ransomware attacks can be devastating from a cost perspective. 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? Due to the unpredictable severity of such attacks, many look to transfer their risk and turn to cyber insurance. Risk transfer can help protect an organization's balance sheet and provide resources if risk mitigation tactics fail.

TRANSFER YOUR RISK. 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.

Incident Response Plan Guidelines

For detailed information on what you should do before, during, and after an attack, download this document. It explains how to create a comprehensive incident response plan that will prevent your organization from being paralyzed by a ransomware attack.



For More Information

Ryan Weber
Public Power & Utility Practice
Marsh USA Inc.
Ryan.weber@marsh.com
281-732-1558

Marsh

Hometown Connections | Partner

About Marsh

A partner of Hometown Connections, Inc., Marsh is the world's leading insurance broker and risk advisor. With around 40,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue over $17 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube, or subscribe to BRINK.

About Hometown Connections, Inc.

Hometown Connections, Inc. is a national, non-profit utility services organization serving community-owned utilities. A single source for many utility products and services, our team of consultants and vendor partners provide affordable and high-quality solutions to help community utilities transform business operations, planning, employee engagement, the customer experience, and much more. Supporting operational and service excellence, all of our services and deliverables are scalable based on the size and objectives of the utility. @HTConnections, Facebook, LinkedIn.

Hometown Connections, AESI-US, Inc., and Marsh USA offer comprehensive cyber and physical security consulting and insurance solutions. Send your inquiry to info@hometownconnections.com for complete information.