RSA

WHITE PAPER

STRATEGIES FOR MANAGING RANSOMWARE RISK IN HEALTHCARE

Ransomware is on the rise across the healthcare industry today, and it's not showing any signs of slowing down soon. The effects to system uptime, loss of profits and irreparable damage to brand reputation for healthcare organizations is just the tip of the iceberg. Today's threats directly impact the patients and their trusted relationships with providers. Everything from patient records and care management to the point-of-care instrumentation used every day to save lives is threatened.

Many healthcare organizations are investing in modernizing their business infrastructures, while expanding their digital ecosystems via third-party tools and partners. Healthcare providers are working as hard as they can to also deploy a host of new technologies, procedures and policies to prevent cyber attacks like ransomware and sustain business continuity if disrupted.

"Ransomware attacks against healthcare providers increased a whopping 350 percent during the last quarter of 2019 with the rapid pace of attacks already continuing throughout 2020."[1]

However, any of these activities, third-party tools and partnerships will expand the attack surface and can be the weak link, exposing healthcare providers to increasing cybersecurity risks that could impede their digital transformation initiatives and other efforts to meet the demands of their customers. Let's take the 21st Century Cures Act, enacted in 2016, as an example. This legislation has an interesting dynamic to it. On one hand, the Cures Act will require more open sharing of patient information to third parties, expanding the threat landscape and potentially making ransomware much more attractive to cybercriminals. On the other hand, if one healthcare organization is held hostage by ransomware, the critical patient information might still be available through another healthcare provider with access to those same shared records. What we do know for sure is that ransomware in healthcare is on the rise. In fact, according to a new report from Corvus, "Ransomware attacks against healthcare providers increased a whopping 350 percent during the last quarter of 2019 with the rapid pace of attacks already continuing throughout 2020."[1]

Ransomware attacks are growing more common in the healthcare industry for a variety of reasons. Today everything is digital, and ransomware blocks the use of computers and databases. Daily hospital routines can be paralyzed, with no new admissions, no patient discharges, and no access to critical patient data. The urgency and criticality of health services from healthcare providers to clients translates into power to get funds more rapidly than other service types. Crisis also puts the victim in a fight-or-flight mode, making the likelihood of payout even greater. Ransomware isn't just a tool for those making cash; it's also often dropped like a grenade on departure to clean up forensic evidence and to create distractions, making it a tool for nation-states too and not just for cybercriminals.

WHY ARE THEY PICKING ON US?

Willie Sutton's famous, apocryphal line when asked why banks are robbed was "because that's where the money is." The reason to go after healthcare is all about the attackers and not the defenders. It could be nation-states looking to not fall behind due to sudden pandemic-related vaccine IP, since that's tied to economic viability or to criminals maximizing ROI.

It was a cold arithmetic that targets the best yield for cyber targeting, and before healthcare it was municipalities and state and local government in the crosshairs. The yield math is now making healthcare more attractive despite stronger defenses

because the money is found in life-or-death situations. Put simply, the rewards are seen by attackers in the results and pull the swarm of hackers in. There are many factors to the continued threats organizations face and it's imperative that we continue to learn and understand them. What we see today is that healthcare information has a longer shelf life in cybercrime underground forums and is selling at a higher premium for a host of reasons. A recent example from the RSA FraudAction™ report shows healthcare records are now selling between $100 and$500.

THE COST OF A RANSOMWARE ATTACK

Given the reputational and regulatory damage a ransomware attack can trigger, it's clear the total cost of ransomware extends far beyond the sum of the ransom. There are the actual costs of recovery of the data and fixing the damage to the network. There are the human costs and potentially lives due to downtime and degradation of service. We see reputational costs with brand, patients, partners and suppliers. Most organizations will certainly face exorbitant compliance, liability, and legal costs and consequences. At the same time, there are morale and HR costs due to burnout and stress of employees. Also, very importantly there is an increased risk as the dark side learns that you are vulnerable and now knows just what buttons to push for another heist.

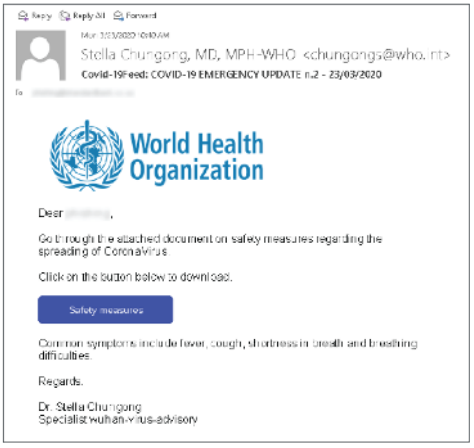
94% of malware is delivered via email" and "phishing attacks accounted for more than 80% of reported security incidents" across industries today.[3]

YOUR STRATEGY FOR MITIGATING THE IMPACT OF RANSOMWARE

RSA recommends a multipronged strategy for addressing ransomware that focuses on prevention through employee training and improved access controls, rapid detection and response, data backup, and building business resiliency.

PREVENTION

Preventing ransomware attacks is not easy, especially for large healthcare organizations. Since so many of these attacks originate as phishing emails, much of prevention hinges on educating your organization's entire workforce, which may number in the hundreds or thousands, to be more aware of these types of attack and the tactics attackers use to perpetrate them. Evidence to support this comes as HIPAA Journal explained that, "Many ransomware attacks are automated and start with phishing emails."[2] Furthermore, a recent article in CSO Online compiled studies and surveys into the current state and found that "94% of malware is delivered via email" and "phishing attacks accounted for more than 80% of reported security incidents" across industries today.[3]


Reply Reply All Forward

Stella Chungong, MD, MPH-WHO <chungongs@who.int>

Covid-19Feed: COVID-19 EMERGENCY UPDATE n.2 - 23/03/2020

World Health Organization

Dear ,

Go through the attached document on safety measures regarding the spreading of Coronavirus

Click on the button below to download.

Safety measures

Common symptoms include fever, cough, shortness in breath and breathing difficulties

Regards.

Dr. Stella Chungong
Specialist wuhan-virus-advisory

Phishing Example From RSA FraudActionTM Intelligence - Threat Report 2020

But phishing isn't the only way ransomware is getting in. Attackers are also exploiting identities and weak passwords. Healthcare services companies have long implemented authorization and access controls as well as multi-factor authentication (MFA) to protect sensitive assets and data. They may need to consider expanding those implementations across the entire organization to protect all access, given the interconnected nature of today's IT infrastructures and how access to one system can quickly lead to others. While traditional authenticators, like hardware tokens, may have been cost-prohibitive and difficult to manage at the scale of a large regional healthcare organization, modern mobile MFA on a smartphone for telehealth purposes is often simpler for users and administrators, and helps to minimize—if not eliminate—organizations' reliance on vulnerable password-based access controls.

Key Takeaway: *Stronger security and access controls combined with training and awareness programs can minimize the human factor risk associated with ransomware.*

RAPIDLY DETECT AND RESPOND TO RANSOMWARE

To lessen the impact from a ransomware attack, healthcare organizations and providers must be able to rapidly detect the malware and prevent it from spreading across the network. This requires deep visibility across networks into endpoints, web applications and other infrastructure (both virtual and cloud-based).

Getting this level of visibility can be difficult for large healthcare organizations with complex IT infrastructures. Arming security operations staff with intelligent security platforms that leverage artificial intelligence to analyze and identify anomalous behavior and malicious code is critical. Ensuring that security operations staff can quickly prioritize and investigate real threats versus spending time analyzing false positives can accelerate mean time to detect and respond. Once a threat is detected, the ability to quickly and automatically orchestrate a security response is essential to minimizing the spread of ransomware and reducing its overall impact.

Key Takeaway: *Organizations will never be able to completely stop the threat of ransomware attacks, so they must have appropriate threat detection and response capabilities to be able to reduce time to detection and automatically orchestrate a response to remediate the threat.*

BACK IT UP

Backup is also a critical component of any ransomware mitigation program. Data should be backed up as close to real time as possible to minimize loss once recovered. Equally important: segmenting data backups from production systems. Organizations absolutely do not want a threat actor to be able to get to data backups, as that will nullify recovery attempts. Organizations should seek out cyber recovery solutions that include policy-driven automated workflows for moving and locking down business-critical data into isolated environments and enabling tools that incorporate artificial intelligence and machine learning analytics methods within a cyber recovery vault. And finally, cyber recovery solutions must be able to automate workflows to perform data recovery and remediation after a cyber incident.

Arming security operations staff with intelligent security platforms that leverage artificial intelligence to analyze and identify anomalous behavior and malicious code is critical.

Consider the impact of data loss on a healthcare organization. If an organization was attacked and unable to recover data after a ransomware attack and became insolvent, loss of sensitive information, the disruption to daily operations, financial losses incurred to restore systems and files, compliance regulatory fines, and the potential harm to an organization's reputation would be devastating.

BUILD RESILIENCY

Recovery from a ransomware incident is essential but insufficient on its own. Given that healthcare providers must operate 24/7, ransomware attacks and the disruptions they cause are pressuring healthcare organizations to move beyond recovery and make resiliency their goal.

Building resiliency requires preventive and risk-driven planning, weaving resilient measures into the organization's business model, aligning security incident response and crisis management, coordinating business and IT recovery, and developing post-disruption strategies to reduce the impact of future disruptions.

Technology also helps to support a rapid response that leads to other important outcomes, such as minimizing disruption to patients, maintaining services and protecting privacy. Organizations must consider their recovery time objective (RTO) as well as the amount of data they can afford to lose. This includes data that the organization and its third parties are generating and potentially losing.

Achieving resiliency also requires practice. Resiliency is earned through drills, from pen testing and red teaming to tabletops and simulations of the whole system. Peacetime is the friend of the forward-leaning healthcare organization to get ready for a crisis.

Key Takeaway: *Preparation and planning are critical elements to minimizing the impact of a ransomware incident. Financial institutions must have a well-documented and exercised business resiliency plan that spans business operations, technology capabilities and risk management to remain resilient in the event of an attack.*

CYBER INSURANCE

Cyber insurance may or may not help you minimize the cost of a ransomware attack. It depends on the policy. Some policies specifically exclude paying the ransom due to the moral hazard. Others will pay it. While cyber insurance can be a huge help to limit financial liability, make sure that it delivers what you think it does and that exception clauses are not invoked. Most importantly, don't use cyber insurance as a substitute for cyber capability and a strong business resiliency plan; it's a great support and financial tool but is no substitute for the right cyber proficiency. For organizations with such policies, CFO magazine explains that "working with the broker and insurers to understand the policy and the procedures for filing a claim is crucial to payment under the policy. Often the policies are tightly drafted to mitigate the impact of cyber fraud and require the policyholder to educate its workforce and implement appropriate means, such as business continuity and disaster recovery procedures, to prevent the ransomware intrusion and mitigate the impacts of an incident."[4]

Building resiliency requires preventive and risk-driven planning, weaving resilient measures into the organization's business model, aligning security incident response and crisis management, coordinating business and IT recovery, and developing post-disruption strategies to reduce the impact of future disruptions.

Key Takeaway: *If your organization chooses to leverage cyber insurance, you must understand the scope and requirements under the policy specific to ransomware in order to clearly acknowledge the level of risk your institution must accept, even with the buttress that the policy provides.*

HOW RSA CAN HELP HEALTHCARE ORGANIZATIONS IMPLEMENT A RANSOMWARE MITIGATION AND OPERATIONAL BUSINESS RESILIENCY STRATEGY

A leader in digital risk management, RSA is helping the world's largest healthcare organizations address ransomware and minimize cybersecurity risks through an integrated risk management program. The RSA portfolio is unique in its ability to bridge security and risk management functions.

A leader in digital risk management, RSA is helping the world's largest healthcare organizations address ransomware and minimize cybersecurity risks through an integrated risk management program.

With respect to preventing and minimizing the impact from a ransomware attack, RSA provides:

- **Modern, mobile multi-factor authentication** through RSA SecurID® Access. This makes it harder for attackers to exploit users' identities or compromised credentials to perpetrate a ransomware attack. RSA SecurID Access also paves the way for a password-less environment that maintains strong security without inconveniencing users.
- **Advanced threat detection and response through RSA NetWitness® Platform**. RSA NetWitness Platform gives security teams the unparalleled visibility they need to detect ransomware and other forms of malware on the network, endpoints, and across virtual and cloud environments. It also provides orchestration and automation capabilities to accelerate response and remediation.
- **An industry-leading integrated risk management platform**. RSA Archer® Suite helps organizations identify, assess and manage a range of risks to their business. It includes a use case for business resiliency that makes it easier for organizations to identify their most critical business processes and technologies, document business resiliency plans, and coordinate a cross-functional response.
- **Prevent fraud in real time with RSA Fraud & Risk Intelligence Suite**, blending risk-based decisioning, predictive analytics, deep entity profiling, modern authentication and global fraud intelligence with the ability to correlate data across anti-fraud tools. RSA FraudAction Intelligence Service monitors dark web forums for potential targeted phishing attacks on your organization.

As a Dell Technologies company, our security and risk management solutions are complemented by Dell Technologies Cyber Recovery Solutions and Services to deliver resilient operations and backup systems that provide quick recovery from ransomware attacks.

Ransomware is a major issue in today's healthcare industry—especially as these institutions rapidly adopt new digital technologies to better serve their patients and compete in the digital era, while adapting to the "next normal" in our brave new connected world. Institutions must understand that there isn't a single silver bullet that can minimize the risk and impact of a ransomware or malware attack. Instead, healthcare organizations must look at a multipronged approach to minimize the opportunity for attack, to be able to rapidly identify when malware is present in the complex and expanding IT environment and be able to remain resilient when the attack occurs. Healthcare organizations will never be immune to cyber attacks and must face the fight on many fronts to protect their reputation of trust with patients and continue to provide access to critical life-enhancing and life-saving services that they rely on.

ABOUT RSA

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change. Find out how to thrive in a dynamic, high-risk world at rsa.com.

1 Reported by Jessica Davis in Health IT Security, xtelligent Healthcare Media, according to Corvus "Ransomware Attacks on Healthcare Providers Rose 350% in Q4 2019". (March 09, 2020)

2 Reported in HIPAA JOURNAL "Advice for Healthcare Organizations on Preventing and Detecting Human-Operated Ransomware Attacks" (April 30, 2020)

3 Reported in CSO online by Josh Fruhlinger "Top cybersecurity facts, figures and statistics for 2020" (March 09, 2020)

4 Michael R. Overly and Aaron Tantleff, CFO.com, "How to Mitigate the Threat of Ransomware," (August 31, 2016)