HEALTH CARE

CASE STUDY: HOSPITAL HIT WITH RANSOMWARE ATTACK—RSM STEPS IN TO HELP

BACKGROUND: A threat is unleashed

While receiving high marks on weekly and monthly security reports from its vendors, an award-winning community hospital with a full-service and acute-care facility serving residents in the Northeast experienced a ransomware incident in the middle of the night. A hospital technician launched his VPN and accessed the workstation remotely to discover some unusual files titled “Sorry.” When clicked, the files triggered an alarming message: “Your systems have been compromised. Follow these instructions.”

When the incident was detected, the hospital's incident response plan activated to alert hospital leadership and response teams that the core information for their electronic medical record (EMR) systems needed for business operations, including telephony, was down. This severely restricted physicians, patients and caregivers in contacting the hospital.

The hospital staff soon realized how dependent they were on the affected systems, and how debilitating a widespread security incident could be. In addition to traditional information technology systems and data, the incident affected elevators, badge swipes, the operators' console, emergency medical services (EMS) integrations, faxing, paging and visitor call routing.

Within the first hour, an incident response team had assembled. The hospital's disaster preparedness and recovery team designated runners to carry ad hoc forms between three different areas to coordinate communications. All functions of the hospital, including operators, emergency department and paramedics needed to be managed without phone service.

The IT team quickly called on anyone with a Wi-Fi access point and used the cellular network to access the community health record and hosted EMR system. They collected new and reimaged laptops and Wi-Fi-enabled devices to access patients' diagnoses, scheduled exams and drug dosages. No patients were rescheduled, though significant needs had to be diverted. Nearly every server and data on most workstations had been encrypted. In total, 50% to 80% of system data was compromised by this ransomware attack. The hosted EMR system had not been compromised by ransomware though access to it had been disabled as a matter of greatest priority.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

How it happened

Upon launch, the ransomware defeated the hospital's anti-virus software. Following that, the hospital's backup system was incapacitated, affecting confidential patient, business and operations data as well as personal computer and shared workstation profiles.

Immediately, cybersecurity insurance was contacted to engage outside resources who would assist in managing the incident. This third-party team searched for the attack origin and followed the compromise. The hack exploited remote access capabilities, a boon for most physicians. Remote access to patient data offers many benefits but also many security challenges. It presents an additional attack channel to patient data; thus, it deserves an additional level of security that was not in place before the incident.

Attackers lurked in the hospital's systems for over 24 hours before the hack, planning their attack. Once they found an administrator account they could use, they escalated their privileges, and pivoted quickly from system to system. Luckily, no data was accessed or acquired, only corrupted or encrypted. Because this hospital had not fully investigated all attack vectors and risks to patient data, it could not see that this scenario was a possibility until it was too late. The hospital's security executive indicated: "It's infrequent that you have to consider the fact that you could be compromised. What would happen if someone gained access? This incident changed our way of thinking."

SOLUTION: RSM helps hospital fortify security

Once the dust settled, the hospital realized they needed to take a closer look at their vulnerabilities and risks, thinking they had a false sense of security with its existing security reports. The hospital contacted RSM to assist in maturing their security program and preparing for future attacks. The following was implemented:

Security testing

RSM performed vulnerability scanning to identify systems or configurations that could be attacked, along with penetration testing, to determine what level of compromise could be achieved by exploiting these vulnerabilities. The RSM team found that the hospital's backup systems were located on the domain, where other providers had assured the hospital team they were not. This meant that the backups (which would typically help an organization recover from ransomware) were also vulnerable to compromise and thus were also affected by the incident. Since then, the hospital has supported and completed a more robust backup solution. To address other weaknesses, they also implemented a multifactor authentication and an identity and access management solution.

TIP: Regular penetration testing and vulnerability scanning are key elements of protecting against compromise. Threat landscapes constantly evolve, and organizations need to regularly evaluate their defenses against these threats. As vulnerabilities are identified, they should be documented in a register that tracks risk and remediation status, owner and due date.

Patching

Vulnerability scans and penetration testing identified some gaps in patch management. Now, a newly instituted maintenance window to install these patches, including scheduled security downtimes, are part of the IT infrastructure at this hospital thanks to RSM's help.

TIP: Missing patches are a prime target for attackers.

Monitoring and alerting

The hospital's security information and event management (SIEM) report showed what appeared to be normal activity, not taking into account the odd hour that the incident occurred. This suggested the SIEM was in need of additional tuning to correlate events that seemed unrelated and innocuous, but together were indicators of compromise. This also emphasized the need to ensure those responsible for reviewing logs and alerts are trained on the SIEM tool as well as initiating the incident response plan as soon as a suspicious event is detected.

TIP: SIEMs should take into account seemingly innocent events; log reviewers should be trained to take action immediately when they become suspicious.

Governance

Acting on the guidance of RSM, the hospital is implementing a formal security governance and security risk management structure.

TIP: If security remains only at the tactical level, systemic issues will not be addressed, critical risks will be overlooked or not prioritized appropriately, and security will not be integrated into business processes. Establishing a formal security governance structure that includes formal security discussions with leaders from a variety of business units will help organizations remain proactive in their security stance.

Budgeting

As RSM suggested, this hospital is incorporating security considerations into budgetary decisions.

TIP: The security executive from this hospital said that budgeting for security should look beyond compliance and regulatory requirements, and added the following:

1. Thin staff and a limited budget cannot get in the way of security improvements. Knowing what your critical risks are will help you prioritize even with limited resources. Ideally, have a budget line specifically for security so that resources can be allocated to these important tasks, rather than eaten up by IT operational needs.
2. Organizations often factor in a reasonable cost and timeline for compliance rather than best practices. While compliance can provide baseline recommendations for implementing security controls, organizations typically need to look beyond compliance in order to truly address their threats.
3. Keep board members in the loop. They should be aware of the reputational and financial risks they are accepting if security is not prioritized.

Roles and responsibilities

RSM continues to help this hospital implement security improvements and a security governance framework to help prevent this type of incident from happening again.

TIP: When assembling a security team, designate a qualified in-house individual (or third party) whose responsibility is to know cybersecurity, and educate him or her on all of your systems. Security tasks often get relegated to a lower-priority status behind IT operational needs, but it is important to designate individuals to items, such as patching, monitoring and incident response. It is difficult to find a single individual who can manage all security tasks, so investigate the use of a third party to augment security efforts.

Contact us to find out how RSM can help your organization protect against ransomware attacks

+1 800 274 3978
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed. RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International. RSM, the RSM logo and *the power of being understood* are registered trademarks of RSM International Association.