WannaCry Impacts and Lessons are Global

5.23.2017

WANNACRY IMPACTS AND LESSONS ARE GLOBAL

"It's gonna hurt bad before it gets better … from my eyes, tonight I want to cry."[1]

C-suite officers around the world have been singing this sad song the last couple of weeks. This has been especially true for any HIPAA covered entity or business that creates, maintains, transmits, or stores unencrypted ePHI. As IT professionals are quick to point out, in the event of a ransomware attack, "there is currently no method of decrypting encrypted files without having the private [decrypt] key."[2] Even if you pay the ransom, however, there is no guarantee that you will receive all the necessary decrypt keys. In many cases, the hackers leave behind a "backdoor"—basically a hidden piece of additional malware that allows the hacker to gain entry at some later time.[3]

The May 12, 2017, massive, international *WannaCry* ransomware attack is a wake-up call for all businesses. In this historic outbreak, malware targeted approximately 300,000 IT systems in 150 countries. Victims included a Renault plant in France, FedEx in the US, Germany's national railway, Deutsche Bahn and the UK's National Health Service. China was hit hard because of the prevalence of pirated software.[4] Russia was hit, too. For any business—but particularly those subject to the HIPAA Privacy and Security Rules—the *WannaCry* attack highlights the importance of basic IT hygiene: keep your IT systems updated and patched. Do not wait for a more convenient time to conduct upgrades—that's why we call these patch warnings "Zero Day Alerts." Hackers are alerted to the vulnerability on the same day that we are. Do not cling to old customized applications that only run on platforms (like Windows XP) that Microsoft no longer supports.

Related Services

Cybersecurity and Privacy Specialty Team

Employee Benefits

Health Care

Health Care Industry Team

Health Information Technology

HIPAA

In the UK alone, 48 medical facilities were infected by the virus, severely compromising patient safety. *WannaCry* ransomware contains an exploit that targets a vulnerability in the Windows SMBv1[5] server to compromise systems, encrypt files, and spread to other hosts. Outdated and unsupported versions of Microsoft were vulnerable to attacks. Although Microsoft issued a patch[6] for the SMB flaw in March, budget constraints, legacy systems, and other business priorities prevented businesses from implementing the software upgrades immediately. Lost in the story was this good news: those companies running current versions of Windows 10 were not vulnerable to this attack.[7]

Prior to the May 12 attack, HIPAA Covered Entities and Business Associates were the most frequent targets of ransomware and malware attacks because of the lucrative resale value of private health records on the black market and the willingness of hospitals and physicians groups to pay ransom — typically in bitcoin—to release systems and information essential to the functioning of critical equipment and information systems, which are truly a matter of "life and death." A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).[8]

As the *WannaCry* attack demonstrates, ransomware can adversely impact all industries. However, due to HIPAA mandates for individuals and entities, ransomware has an especially devastating impact. In addition to the "world of hurt" that results from the interruption of healthcare operations, HIPAA fines, penalties and breach notification requirements, and the collateral effects of the attack (*i.e.*, public relations costs, litigation, *etc.*) that inevitably follow ratchet up the pain of remediating a ransomware attack. Noncompliance with the HIPAA Security Rule can further impact the resulting pain associated with a security breach.

The HIPAA Security Rule simply establishes a floor for the security of ePHI; those subject to its reach are encouraged to implement additional, more stringent security measures. The Security Management Process of the Security Rule requires that covered entities and business associates undertake periodic (at least annually) risk assessments and implement security measures sufficient to reduce those identified risks and vulnerabilities to a *reasonable* and *appropriate* level. Because ransomware denies access to data, maintaining frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack. It is also critical that the backup has no active connection to the live IT environment, or it too can become encrypted by a ransomware attack. Implementing a data backup plan is a Security Rule requirement for HIPAA covered entities and business associates as part of maintaining an overall contingency plan.

HIPAA also requires Security Incident (as defined by HIPAA) procedures, including procedures for responding to and reporting Security Incidents. Under the HIPAA Security Rule, the presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a "Security Incident." More importantly, however, is the fact that the presence of ransomware or malware in an entity's system can elevate to a reportable HIPAA breach if "the acquisition, access, use, or disclosure of PHI is in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI." [9] Although a ransomware attack was subject to much debate as to whether it qualified as a reportable breach, in a July 2016 Guidance, the OCR definitively settled the

issue with a resounding "Yes." According to the OCR, "[w]hen electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule."

Just days after the *WannaCry* attack, HHS/OCR Senior Advisor for HIPAA Compliance and Enforcement, Iliana Peters, reiterated the OCR's position on ransomware, discussing how *WannaCry* and its copycats can trigger reportable breaches. As detailed in the Guidance, a ransomware attack is presumed to be a data breach and only if a Covered Entity or Business Associate can demonstrate, through a credible risk assessment, that there is a "...low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, will that presumption be overcome. Where ransomware has taken hostage of an entity's ePHI, it is unlikely the presumption of a breach will abate, triggering the Covered Entity's compliance with the Breach Notification rules.[10]

The *WannaCry* attack demonstrates the need for proper HIPAA compliance, at a minimum. Healthcare providers, group health plans and their business associates should learn from *WannaCry* and ensure their continued HIPAA compliance. At a minimum, attention must be paid to following tasks:

- ***Conduct a Security Risk Assessment immediately*** to identify unsupported software systems vulnerable to cyberattacks, in particular old versions of Microsoft Windows (see footnote 4 above). Microsoft posts free patches. Establish a regular day/time to download them.[11] Review other systems and do patch risk assessments. Segregate all legacy systems that are unsupported (and thus not "patchable"). Vulnerability testing—internal and external—should be included in any risk assessment to identify areas in the system that can be gateways for malware.
- ***Assess your back-up and recovery plans***. Test your backup and recovery plan. Check the ICS-CERT Alerts https://www.us-cert.gov/ncas/alerts to keep abreast of news and security warnings. The need for segregated back-up systems is clear when ransomware encrypts your system. When a solid back-up plan is in place, the consequences of a ransomware attack on an entity's system is minimal—it need only turn to the back-up to continue operations.
- Covered Entities must ensure their Business Associate Agreements are updated and in place and that their Business Associates and any downstream contractors are in compliance with applicable HIPAA Rules. Request copies of employee training conducted and risk assessments performed, as well as any remedial actions taken. Covered Entities must obtain reasonable assurance that their ePHI in the hands of a Business Associate or other authorized third party is protected from cyber events.
- ***Train your workforce.*** Make sure that your entire workforce has sufficient training (at least annually) and education about security and, in particular, ransomware. While there may be patches to help alleviate the risks of ransomware, there are no patches for human error.
- ***Review insurance policies*** for cyber-event insurance coverages, including coverage for damages including the costs of breach notification expenses and remediation activities and costs.

Security Risk Assessments can be daunting, but they are not only appropriate for continuity of system operations, they are mandatory for maintaining the security of the information in those systems. With the increased enforcement activity by OCR and increased liability for non-compliance, having a solid and up-to-date Security Management Plan is a must. Organizations that are unwilling or unable to undertake the time and expense in doing risk assessments and funding software and equipment upgrades, are placing themselves at risk for not only cyber attacks but OCR Enforcement. Simply having a risk management plan that addresses how to obtain bitcoins to pay ransom to get your data back[12] is not sufficient to meet the demands of HIPAA and many other privacy regulations.

The attorneys in Butzel Long's, cybersecurity, healthcare law, and employee benefits groups stand ready to help our clients and friends meet their HIPAA needs. Please feel free to contact any of the attorneys below or your Butzel Long attorney contact if we can provide additional information or assist you with the matters discussed in this Alert.

Debra A. Geroux
248.258.2603
geroux@butzel.com

Susan Patton
734.213.3432
patton@butzel.com

Claudia Rast
734.213.3431
rast@butzel.com

---

[1] Keith Urban, *Tonight I Wanna Cry*.

[2] https://www.us-cert.gov/ncas/current-activity/2017/05/17/ICS-CERT-Releases-WannaCry-Fact-Sheet.

[3] All is not lost, however: an experienced forensic team can locate and neutralize those "backdoor" traps.

[4] Pirated software is not registered, so it cannot be patched.

[5] *WannaCry* employed an exploit dubbed "EternalBlue" that was allegedly crafted by the NSA, and used for the past five years. http://wapo.st/2rAhrdw. This exploit was posted to the Internet by a group called Shadow Brokers last month. EternalBlue exploits a vulnerability in the Server Message Block (SMB) of all unpatched versions of Microsoft (Windows XP, Windows 8, and Windows Server 2003). Only Windows 10 was not vulnerable.

[6] MSFT, Tech30.

[7] The bad news continues, however, as hackers are reported to have enlisted scores of "zombie" devices such as webcams, modems, and other unsecure devices to funnel traffic via DDoS attacks at the web address created as the "sinkhole" that effectively cut short the impact of the WannaCry attack. If the DDoS attack knocks the sinkhole offline, some of the dormant WannaCry infections may reactivate.

[8] United States Government Interagency Guidance Document, *How to Protect Your Networks from Ransomware*, available at https://www.justice.gov/criminal-ccips/file/872771/download.

[9] 45 C.F.R. 164.402.

[10] Iliana Peters, Georgetown Law's Cybersecurity Law Institute, May 17, 2017.

[11] Always use caution to confirm that the patch will "play well" with your legacy systems.

[12] http://www.coindesk.com/information/how-can-i-buy-bitcoins/