LATHAM&WATKINS

Client Alert
Commentary

Latham & Watkins Information Law, Data Privacy & Cybersecurity and Healthcare & Life Sciences Practices

July 10, 2017 | Number 2172

How Can Healthcare Organizations Prepare for the Next Cyberattack?

HHS OCR issues checklist, iterative guidance in wake of WannaCry and Petya attacks; Anthem breach settlement provides additional lessons.

Key Points:

- Healthcare organizations are particularly vulnerable to ransomware attacks, which are becoming more frequent and more sophisticated.
- The US Department of Health & Human Services has issued new guidance in response to the increased risk of ransomware and other cyberattacks in order to help Covered Entities and Business Associates better prepare.
- Recent enforcement matters and the Anthem data breach settlement also provide takeaways for all healthcare organizations to help shore up compliance with laws and regulations.

On June 2, 2017, in the wake of the widespread cyberattack caused by the WannaCry ransomware cryptoworm, the US Department of Health & Human Services (HHS), Office for Civil Rights (OCR) added to its arsenal of cybersecurity guidance a checklist to assist HIPAA Covered Entities and Business Associates in responding to cyber-related security incidents (the Cybersecurity Checklist).[1] The Cybersecurity Checklist focuses on entities' execution of their incident response plans as well as external reporting obligations, and encourages entities to perform certain mitigating efforts, including sharing information with private-sector information-sharing and analysis organizations (ISAOs). In addition, recent OCR enforcement matters and the June 23, 2017 Anthem breach settlement provide lessons for all regulated healthcare organizations in what is required for compliant breach preparedness.

Understanding Ransomware Attacks

Ransomware is a unique type of malicious software, or malware, that is used to deny a user access to systems or data. HHS has described ransomware as malware that "exploits human and technical weaknesses to gain access to an organization's technical infrastructure in order to deny the organization access to its own data by encrypting that data."[2] While recent attacks have grown exponentially in reach and sophistication, ransomware historically has first infected organizations through spearphishing emails, which use social engineering methods to induce the recipient to click on a link that in reality loads malware onto the user's computer. The malware then holds the affected organization's systems or data hostage by encrypting data, and demanding a ransom payment to unlock the user's access to their own information. According to the security firm Kaspersky, ransomware attacks in the first quarter of 2017 had risen to 218,625, compared with 61,832 attacks in the last quarter of 2016, representing an increase of

250%.[3] In the last two months alone, two separate global cyberattacks relying upon weaponized versions of ransomware have affected organizations worldwide.

In May 2017, the WannaCry strain of ransomware (also known as Wanna Decryptor, WannaCrypt, and WCry), infected more than 300,000 computers in more than 150 countries.[4] WannaCry likely started through spearphishing emails, where an employee clicked on an infected link, such as a malicious Microsoft Word file, to enable the ransomware. However, once enabled, the ransomware could then spread through the organization's entire network, making WannaCry the world's first "ransomworm," according to Lee Kim, director of privacy and security for Healthcare Information and Management Systems Society (HIMSS) North America, a non-profit focused on better health through information technology.[5] Upon infecting a computer, WannaCry encrypted the computer's files, rendering them unreadable to the user, and demanded $300 in Bitcoin for unlocking encrypted files, with the price doubling after three days. WannaCry threatened to delete all encrypted files if the ransom wasn't paid in a week.

WannaCry exploited a vulnerability in Microsoft Windows called EternalBlue that the National Security Agency (NSA) had discovered. The hacker group known as the Shadow Brokers leaked EternalBlue to the internet in April 2017. Microsoft had issued a software update in March 2017 for its most recent operating systems that protects against exploitation of this vulnerability, but some organizations and users had not implemented the patch or were running old Windows operating systems for which the patch was not made available. After news of the attack hit, Microsoft released an additional emergency patch, taking the unprecedented step of providing direct support for unsupported operating systems, like Windows XP.

And just at the end of June, a new malware attack known as Petya (and also known as NotPetya, PetrWrap, or GoldenEye) hit companies in various countries around the world.[6] Like WannaCry, the malware used the EternalBlue exploit, allowing it to spread quickly to infected systems. The damage was worst in Ukraine where the attack is believed to have started. Unlike a traditional ransomware attack, the motivation does not appear to have been financial gain but instead destruction of the infected systems.[7] The Petya attack is known to have affected healthcare providers and pharmaceutical companies in the US. In particular, the attack crippled information technology operations at two Pennsylvania providers, Sewickley-based Heritage Valley Health System and the Association of Specialty Physicians, an independent medical group in Beaver.[8]

WannaCry appeared to disproportionately affect healthcare providers, most notably the UK's National Health Service (NHS). Hospitals and other healthcare providers — and their extensive supply chain of device manufacturers, laboratories, and other critical goods and services — are particularly desirable targets for ransomware attackers for several reasons. First, patient care will rarely if ever be viewed as an acceptable trade-off, as the choice is often a matter of life and death. Secondly, hospitals and healthcare providers are vulnerable when they have out-of-date systems, and in fact, the industry is known for not investing as much in resources as other industries on key data security steps such as patching and updating firmware and software, according to a 2015 KPMG report.[9] Information technology experts believe it is unlikely that hospitals were targeted by the WannaCry attackers — rather, "they were simply more prone to the malware."[10] In this instance, US health organizations were largely spared, likely due to the advance warning of the cyberattack and the available patch received from the attacks in Europe, as well as the "kill switch" fortuitously discovered by a researcher in the United Kingdom.[11] While US hospitals appear to have largely avoided the attack, medical devices seem to have been particularly vulnerable.[12] Nevertheless, experts warn that malware attacks can morph and change, and that "overall the healthcare industry is particularly vulnerable to ransomware and is a high-priority target for cybercriminals because of the high value of health data."[13]

OCR's Iterative Guidance Emphasizes Preparation and Mitigation

In May 2017, OCR issued guidance on cyberattacks (the 2017 OCR Guidance), emphasizing the importance of implementing an incident response plan that creates a "roadmap for implementing the entity's incident response capabilities," and allows for a "proper, concentrated, and coordinated approach" to incident response.[14]

In the Cybersecurity Checklist, OCR highlights the importance of mitigation efforts, noting that it considers all mitigation efforts taken by a Covered Entity or Business Associate during any particular breach investigation. Mitigation efforts include voluntary sharing of breach-related information with law enforcement agencies and other federal organizations and ISAOs.

HHS has also helpfully updated its July 2016 ransomware guidance (the 2016 OCR Guidance), following the recent WannaCry attack. OCR had noted in the July 2016 that a ransomware attack will be presumed to be a reportable breach, unless an entity can demonstrate, by performing and documenting a multi-factor risk assessment, that there is a low probability of compromise to the Protected Health Information (PHI).[15] Following the WannaCry attack, in email messages to its OCR-PRIVACY-LIST listserv,[16] OCR clarified the 2016 OCR Guidance by stating:

> "If the data is not encrypted by the [Covered Entity or Business Associate] to at least NIST [National Institute for Standards and Technology] specifications when the ransomware attack is deployed, then OCR presumes a breach occurred, due to the ransomware attack. As such, the [Covered Entity or Business Associate] would need to prove, through forensic or other evidence, that the ePHI [Electronic Protected Health Information] was encrypted when the attack occurred, and the ransomware containerized (or encrypted again) already-encrypted ePHI."[17]

This statement usefully makes clear that encryption "to at least NIST specifications"[18] provides a so-called "safe harbor" in the event of a presumed breach by ransomware attack. That is, while a ransomware attacker is presumed to have committed an unauthorized acquisition of PHI that compromises the security or privacy of the PHI, where the PHI can be affirmatively shown to have been unreadable to the attacker (*i.e.,* the attack has not also compromised encryption keys or other means to read data), a "breach" has not occurred. Notably, in the case of a ransomware attack, the breach is still presumed, but Covered Entities and Business Associates can now rely on the presence of encryption to the NIST specifications as a definitive mitigating factor to weigh against the presumption of a breach. This is consistent with the language and intent of the HIPAA Breach Notification Rule, which only requires notification in the case of an unauthorized acquisition, access, use, or disclosure of PHI that is not encrypted (that is, not rendered unusable, unreadable, or indecipherable to unauthorized persons through a technology or methodology specified under the NIST guidelines).[19]

In the 2016 OCR Guidance, OCR listed other steps or circumstances that may be relevant to rebutting that presumption, including:

- Implementing robust contingency plans, including disaster recovery and data backup plans
- Conducting frequent backups and ensuring the ability to recover data from backups
- Determining, through a "thorough and accurate evaluation of the evidence acquired and analyzed," the exact type and variant of malware, the algorithmic steps undertaken by the malware, and the exfiltration attempts by the hackers

For a detailed analysis of the 2016 OCR Guidance, see the Latham & Watkins *Client Alert*, Ransomware Attacks: When Is Notification Required?

Collaboration Is Key

In an effort to prevent widespread cyberattacks like WannaCry, OCR has encouraged Covered Entities and their Business Associates, as part of their mitigation efforts, to share information about a breach event (excluding any potentially affected PHI), with federal agencies such as the Department of Homeland Security and the HHS Assistant Secretary for Preparedness and Response, as well as private-sector Information Sharing and Analysis Organizations (ISAOs). In addition, OCR has encouraged healthcare providers whose facility has experienced a suspected cyberattack affecting medical devices to contact the US Food & Drug Administration (FDA)'s 24/7 emergency hotline.[20] While not expressly required under HIPAA, OCR encourages entities to share "cyber threat indicators," noting in the 2017 OCR Guidance that it is "more important than ever for organizations to work together during incident response."

The Cybersecurity Information Sharing Act of 2015 (CISA) describes "cyber threat indicators" as information that is necessary to describe or identify:

- Malicious reconnaissance
- Methods of defeating a security control or exploitation of a security vulnerability
- A security vulnerability
- Methods causing a user with legitimate access to defeat a security control or exploit a security vulnerability
- Malicious cyber command and control
- A description of actual or potential harm caused by an incident
- Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law, or
- Any combination thereof[21]

As noted above, OCR would consider such voluntary sharing of information with DHS, HHS, FDA, or ISAOs to be a mitigation effort during a breach investigation. However, OCR rightly cautions that sharing breach-related information with other federal agencies "does not constitute inadvertent or intentional reporting to OCR," and does not take the place of any required notification to OCR under the HIPAA Breach Notification Rule.[22] Covered Entities, Business Associates, and other regulated entities should also avoid the risk of over-reporting cyberattacks, which could place them in the crosshairs of regulators who may treat them as "perpetrators that allowed a breach of their customers' data," as opposed to law enforcement who treat them as crime victims.[23]

Post-Breach Enforcement Risks: Lessons of Recent Breach Resolutions with HHS and NAIC

On Friday, June 23, 2017, Anthem Insurance Companies, Inc. (Anthem) announced that it will pay US$115 million to settle the multidistrict class action ligation relating to the 2015 cyberattack that exposed personal information of more than 78 million individuals. According to a January 6, 2017 press release issued by the California Department of Insurance, the data breach began on February 18, 2014, as a result of a phishing email that, once opened, permitted the user's computer to download malicious files and also allowed hackers to gain remote access to that computer, as well as a number of other Anthem systems, including Anthem's data warehouse.[24] In December 2016, Anthem reached a joint settlement with members of the National Association of Insurance Commissioners (NAIC) relating to the 2015 cyber breach, which required Anthem to, among other things, implement a number of enhanced security measures and continue cybersecurity monitoring (NAIC Settlement Agreement). Even though the NAIC-led investigation found that Anthem's pre-breach cybersecurity was "reasonable and included the implementation of technologies and procedures consistent with or exceeding those of a typical organization of its size and type," and Anthem had already incurred US$115 million of costs relating to security improvement, Anthem still agreed to make a number of enhancements to its information security systems as part of the NAIC Settlement Agreement.

In recent enforcement actions, OCR has increasingly focused on the affected organization's security compliance programs, including particularly the sufficiency of an entity's enterprise-wide security risk analysis and the implementation of a subsequent risk management plan to address any identified risks and vulnerabilities to the entity's ePHI. As noted in the 2016 OCR Guidance, compliance with the HIPAA Security Rule can prevent the introduction of malware, including ransomware.

On April 24, 2017, OCR announced a settlement for potential HIPAA violations with a wireless health services provider, CardioNet, including US$2.5 million Resolution Amount and a Corrective Action Plan (CAP). CardioNet reported an employee's stolen laptop to OCR in January 2012, which resulted in the impermissible disclosure of ePHI of 1,391 individuals. OCR's investigation indicated that CardioNet had insufficient risk analysis and risk management processes in place when the laptop was stolen. While CardioNet had policies and procedures in draft form, they had not yet been implemented.

On April 12, 2017, OCR announced a settlement for potential HIPAA violations with Metro Community Provider Network (MCPN), a federally qualified health center based in the greater Denver, Colorado metropolitan area, which had experienced a phishing event in 2012 when a hacker accessed employees' email accounts and obtained 3,200 individuals' ePHI. MCPN paid a US$400,000 Resolution Amount and entered into a CAP with OCR. OCR noted that MCPN failed to implement a security management process to safeguard such ePHI. OCR's investigation indicated that MCPN had not conducted a risk analysis to assess the risks and vulnerabilities in its ePHI environment and therefore did not implement a corresponding risk management plan to any such risks and vulnerabilities that would have been identified through such a risk analysis. OCR further noted that subsequent risk analyses conducted by MCPN were insufficient to meet HIPAA Security Rule requirements.

Similarly, on November 22, 2016, OCR announced a settlement for potential HIPAA violations with the University of Massachusetts Amherst (UMass), including a US$650,000 Resolution Amount and CAP. On June 18, 2013, UMass had reported to OCR that one of its workstations had become infected with malware, resulting in the impermissible disclosure of ePHI of 1,670 individuals. UMass determined that the malware had gained access to its ePHI because no firewall was in place. OCR's investigation indicated that UMass did not conduct an "accurate and thorough risk analysis" until September 2015 and failed to ensure that firewalls were in place.

How to Prepare for the Next Cyberattack

- **Vulnerability Patching**: The key takeaway from the WannaCry cyberattack is that patch management policies deserve the highest priority, as well as ensuring adequate staffing and resources to carry out this work. While the HIPAA Security Rule does not specifically address vulnerability or patch management, firewalls, or monitoring of inbound and outbound traffic, appropriate risk management will in turn mandate close adherence to these prevailing security practices. Therefore, the senior executives of any regulated healthcare organization should require formal, documented patch management policies, and regular reporting on whether they are being followed in practice. IT staff must remain up to date on available patches created to correct known software security vulnerabilities and, when appropriate, promptly apply patches to the organization's computer systems after testing. However, older systems running on outdated (unsupported) operating systems and end-of-life applications require equal attention. In 2014, the Anchorage Community Mental Health Service paid OCR a US$150,000 Resolution Amount as part of a settlement for potential HIPAA violations, including a failure to apply software patches that had contributed to a 2012 malware-related breach affecting more than 2,700 individuals. As *The Wall Street Journal* has noted, "organizations that use mission-critical software, such as hospitals … often have no choice but to use outdated operating systems. In fact, it can be disastrous for them to patch their computers when an update becomes available" because software could cease to function, affecting patient care.[25] For these organizations, compensating controls — which can be discovered and addressed through a Risk Analysis and Risk Management Plan, as described below — are vitally important to have.

- **Risk Analysis:** Enterprise-wide risk assessments should occur annually, at a minimum, as an expected best practice. Successful HIPAA compliance requires a common-sense approach to assessing and addressing the risks to ePHI on a regular basis. This includes reviewing systems for unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks. HHS has also flagged email (anti-phishing measures and training) as a key risk area for hospitals, as email attachments commonly deliver malware.

- **Risk Management Plan:** Healthcare organizations should implement a plan for categorizing threat-vulnerability pairings identified by the Risk Analysis, and for prioritizing remediation of pairings that create the highest risk to the organization. With ransomware widely known as a top threat, backup and recovery plans will fall under close scrutiny. Paying a ransom to avoid impacts to patient care may seem a reasonable trade-off and even be the best option; however, as a follow-on matter, regulators may very well investigate and question why a payment was necessary at all. Redundancy and rapid restore capabilities are expected for systems and operations critical to patient care. Healthcare organizations should consider whitelisting applications, segmenting networks and back-up systems, and taking other basic steps to prevent the rapid spread of malware within the organization.

- **Cybersecurity Incident Response Plan:** Healthcare organizations should update their incident response plans to reflect specific threats — including nation- state attacks, hacktivists, ransomware, insiders, and inadvertent data leakage, among others — and to itemize internal and external reporting obligations. This provides decision makers with a documented roadmap for a timely and compliant response in a crisis. Many healthcare organizations are quite experienced and efficient with breach notification to individual affected patients and HHS, but are less rehearsed or prepared to handle major operational disruptions that flow from ransomware and other types of cyberattacks. Healthcare organizations should make sure their plans have the right breadth and depth for multiple scenarios.

- **Training:** Healthcare organizations should train their workforce members to understand the warning signs of cyberattacks and should ensure that workforce members are familiar with internal reporting obligations. Over-training against phishing attacks is probably not possible.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Stuart S. Kurlander
stuart.kurlander@lw.com
+1.202.637.2169
Washington, D.C.

Heather B. Deixler
heather.deixler@lw.com
+1.415.395.8110
San Francisco

Susan Ambler Ebersole
susan.ebersole@lw.com
+1.202.637.1016
Washington, D.C.

Elizabeth N. Purcell
elizabeth.purcell@lw.com
+44.20.7710.5801
London

You Might Also Be Interested In

New Executive Order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"

Ransomware Attacks: When Is Notification Required?

Keeping Your Company's Data Safe This Tax Season

NYSDFS Revises Cybersecurity Rules to Accommodate Industry Concerns

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham's *Client Alerts* can be found at www.lw.com. If you wish to update your contact details or customize the information you receive from Latham & Watkins, visit http://events.lw.com/reaction/subscriptionpage.html to subscribe to the firm's global client mailings program.

Endnotes

[1] HEALTH AND HUMAN SERVICES, OFFICE FOR CIVIL RIGHTS, MY ENTITY JUST EXPERIENCED A CYBER-ATTACK! WHAT DO WE DO NOW? (2017), available at https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf (Cybersecurity Checklist).

[2] HEALTH AND HUMAN SERVICES, OFFICE FOR CIVIL RIGHTS, FACT SHEET: RANSOMWARE AND HIPAA (2016), available at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (2016 OCR Guidance).

[3] Roman Unuchek, Fedor Sinitsyn, Denis Parinov, Vladislav Stolyarov, *IT threat evolution Q1 2017. Statistics*, SECURELIST.COM (May 22, 2017, 9:03 AM), available at https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/.

[4] *See* Rob Sloan, *A Response Checklist*, in WSJ PRO CYBERSECURITY, THE WANNACRY CYBERATTACKS: DEALING WITH THE RISKS (2017).

[5] Greg Slabodkin, *Few U.S. Healthcare Organizations Affected by WannaCry*, HealthDataManagement.com (May 16, 2017, 7:09 AM), available at https://www.healthdatamanagement.com/news/us-healthcare-organizations-appear-to-dodge-wannacry-bullet.

[6] Robert McMillan, David Gauthier-Villars, and James Marson, *Cyber Attacks Hit Major Companies Across the Globe*, WSJ.com (June 27, 2017, 8:24 P.M.), available at https://www.wsj.com/articles/cyberattacks-hit-global-companies-in-europe-1498575793.

[7] Joe Uchill, *Massive ransomware attack not actually ransomware: report* (Jun. 28, 2017 1:25 P.M.), available at http://thehill.com/policy/cybersecurity/339860-massive-ransomware-attack-not-actually-ransomware-report?utm_source=&utm_medium=email&utm_campaign=9523.

[8] Melanie Evans, *Cyberattack Causes Some Surgeons to Cancel Operations*, WSJ.com (June 28, 2017, 5:55 P.M.), available at https://www.wsj.com/articles/cyberattack-causes-surgeons-to-cancel-some-operations-1498686899.

[9] Greg Bell & Michael Eber, *Health Care & Cyber Security: Increasing Threats Require Increased Capabilities*, KPMG.com (2015), available at https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf.

[10] Adam Janofsky, *For Some Organizations, Patching Isn't an Answer*, in WSJ Pro CyberSecurity, The WannaCry Cyberattacks: Dealing with the Risks (2017).

[11] *See* Trend Micro, *Massive WannaCry/Wcry Ransomware Attack Hits Various Countries*, BLOG.TRENDMICRO.COM (May 12, 2017, 1:39 PM), available at http://blog.trendmicro.com/trendlabs-security-intelligence/massive-wannacrywcry-ransomware-attack-hits-various-countries/.

[12] *See* Thomas Fox-Brewster, *Medical Devices Hit for the First Time in US Hospitals*, FORBES.COM (May 17, 2017, 9:00 AM), available at https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#4a87a972425c.

[13] Greg Slabodkin, *Few U.S. Healthcare Organizations Affected by WannaCry*, HEALTHDATAMANAGEMENT.COM (May 16, 2017, 7:09 AM), available at https://www.healthdatamanagement.com/news/us-healthcare-organizations-appear-to-dodge-wannacry-bullet.

[14] HEALTH AND HUMAN SERVICES, OFFICE FOR CIVIL RIGHTS, CYBERSECURITY INCIDENTS WILL HAPPEN… REMEMBER TO PLAN, RESPOND AND REPORT! (2017), available at https://www.hhs.gov/sites/default/files/may-2017-ocr-cyber-newsletter.pdf (2017 OCR Guidance).

[15] 2016 OCR Guidance.

[16] To subscribe to this listserv, visit https://list.nih.gov/cgi-bin/wa.exe?SUBED1=OCR-PRIVACY-LIST&A=1.

[17] HHS Update #4: International Cyber Threat to Health Care Organizations, dated May 17, 2016, available at https://list.nih.gov/cgi-bin/wa.exe?A2=ind1705&L=OCR-PRIVACY-LIST&F=&S=&X=8BB672EFA06311B957&P=6618 (password protected for subscribers only).

[18] Consistent with the *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, issued by the Secretary of HHS under section 13402(h)(2) of Public Law 111-5, PHI is rendered unusable, unreadable, or indecipherable to unauthorized persons if it has been encrypted under (1) a valid encryption process for data at rest consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices; or (2) a valid encryption process for data in motion which complies, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

[19] HIPAA Breach Notification Rule at 45 C.F.R. §§ 164.402-410.

[20] HHS ASPR/CIP HPH Cyber Notice: Current International Ransomware Campaign, dated June 28, 2017, available at https://list.nih.gov/cgi-bin/wa.exe?A2=OCR-PRIVACY-LIST;9151234a.1706 (password protected for subscribers only).

[21] Cybersecurity Information Sharing Act (CISA) of 2015, Pub. L. No. 114–113, div. N, §§ 103, 105, 129 Stat. 2935, 2939-40, 2943-50 (codified at 6 U.S.C. §§ 1502, 1504).

[22] HHS Update #4: International Cyber Threat to Health Care Organizations, dated May 17, 2016, available at https://list.nih.gov/cgi-bin/wa.exe?A2=ind1705&L=OCR-PRIVACY-LIST&F=&S=&X=8BB672EFA06311B957&P=6618 (password protected for subscribers only).

[23] Kate Fazzini, *Ransomware Presents Complex Compliance Risks*, in WSJ Pro CyberSecurity, The WannaCry Cyberattacks: Dealing with the Risks (2017).

[24] Investigation of major Anthem cyber breach reveals foreign nation behind breach, dated Jan. 6, 2017, available at http://www.insurance.ca.gov/0400-news/0100-press-releases/2017/release001-17.cfm.

[25] Adam Janofsky, For Some Organizations, Patching Isn't an Answer, in WSJ Pro CyberSecurity, The WannaCry Cyberattacks: Dealing with the Risks (2017).