

Morgan Lewis

FAST BREAK:

***SECURITY BREACH CRISIS
RESPONSE***

Reece Hirsch
Mark Krotoski
Jake Harper
June 22, 2017

Agenda

- Implementing an effective security breach response plan
- Lessons to be learned from recent OCR enforcement actions
- What the HIPAA Phase 2 audits can tell us so far about OCR's breach response expectations
- OCR's cyber-attack quick-response checklist
- OCR's ransomware guidance
- Responding to the threat of ransomware such as WannaCry
- Coordinating with law enforcement when responding to a breach

Healthcare Industry in the Crosshairs

- Healthcare, like financial services, is one of the industries that is most extensively regulated with respect to privacy and cybersecurity
- That does not mean that the industry is adequately prepared to defend against cyber threats
- Large, high-profile cyber attacks are increasingly targeting healthcare organizations
 - Anthem – 78.8 million individuals affected
 - Premera Blue Cross – 11 million individuals affected
 - UCLA Health System – 4.5 million individuals affected
 - All hacking/IT incidents
- FIN4 malware attacks
- Ransomware attacks aimed at hospitals

2016 Ponemon Healthcare Study

- Ponemon Institute's 2016 Sixth Annual Benchmark Study on Privacy and Data Security of Healthcare Data
 - 89% of healthcare organizations reported at least one data breach in the last two years
 - 45% had more than 5 breaches
 - “Criminal attacks” are the root cause of most data breaches
 - This category has consistently increased in recent years
 - Other root causes of breach:
 - Third party snafu
 - Stolen devices
 - Malicious insiders

The Cost of Healthcare Breaches

- Ponemon Institute's 2016 Healthcare Study also found:
 - The average cost of a healthcare breach for healthcare organizations (HIPAA covered entities) over the past two years – estimated to be more than \$2.2 million
 - The average cost of a data breach to business associates over past two years – more than \$1 million
- Nevertheless, half of all organizations have little or no confidence that they can detect all patient data loss and theft
- Slight increased investment over past year in technology, privacy and security budgets
- But the majority of healthcare organizations still don't have adequate security budget to curtail or minimize data breach incidents

Incident Response Plans

- Security incident response plans are a focus for both covered entities and business associates under the ongoing HIPAA Phase 2 audits
- Documenting and implementing a comprehensive incident response plan is one of the best things that an organization can do to improve its HIPAA compliance posture
 - Reduces risk of investigation
 - Responsive to HIPAA Phase 2 audits
 - Mitigates substantial damages that may arise from a significant and poorly managed breach

The Incident Response Plan Is an Enterprise-Wide Document

- A key component of a security compliance program is an incident response plan
- Typically developed as a stand-alone module distinct from security policies and procedures
 - Don't confuse it with security incident procedures under Section 164.38(a)(6) of the HIPAA Security Rule
 - Addresses applicable HIPAA Breach Notification Rule requirements, including documentation of breach risk assessments
 - More than just a technical, systems document, requires input from legal, compliance and others
 - Includes employee-facing components

An Effective Incident Response Plan

- An effective incident response plan should:
 - Establish an incident response team with representatives from key areas of the organization
 - Identify necessary external resources in advance (forensic IT consultant, mailing vendor, call center operator, credit monitoring service)
 - Provide for training of rank-and-file personnel to recognize and report security breaches
 - Outline media relations strategy and point person

Meet During Peacetime

- No incident response team should be forced to learn their roles on the fly during a breach
 - Meet in peacetime
 - Understand the steps outlined in the breach response plan and each team member's role and responsibility
 - Run scenarios in advance
 - What does your company's worst-case scenario look like?
 - Is your company protected from potential breach liabilities through indemnification? Cyberliability insurance?
 - How likely is it that breach damages might exceed contractual limitations of liability? Insurance liability limits?
- If your organization doesn't have an IRT that meets regularly to discuss cyber threats and incident response, then that should be viewed as a cybersecurity compliance red flag

Training

- Incident response plan should include a module that is shorter and directed to employees
 - Can form the basis for regular training (once a year is advisable)
 - Employees should be able to recognize the significance of a breach when it occurs and report it promptly to supervisors
- Discovery of a breach by an employee may be imputed to the organization
 - Clock begins ticking for notification of affected individuals
 - HIPAA recognizes this form of constructive knowledge

Cyberliability Insurance

- We've seen some cyberliability insurance carriers question a covered entity's determination of whether a breach has occurred under HIPAA's "low probability of compromise" standard
- When the facts of a breach incident are unclear, covered entities often have an interest in erring on the side of caution by notifying
 - Cyberliability insurance carriers often have an interest in not paying a claim
- If your carrier is not willing to accept your reasonable risk assessment regarding whether an incident constitutes a breach, then you should consider finding another carrier
- Does your cyberliability insurance policy cover damages related to ransomware attacks, such as ransomware payments, investigation costs and remediation after the attack?

Recent OCR Enforcement Actions

- January 9, 2017: \$475,000 settlement with Presence Health Network, one of largest Illinois health systems
 - First time OCR enforcement action has been based on failing to comply with breach notification requirements
 - Paper-based operating room records of 836 patients went missing
 - Presence failed to comply with 60-calendar-day breach notification timing standard
 - Notified OCR 101 days after discovery, individuals (104 days), media (106 days)
 - Don't delay notification because investigation of the breach is still uncovering new information
 - OCR breach notification process permits an addendum notification
 - Each day notification is late is a separate violation of the Breach Notification Rule!
- April 24, 2017: Settlement agreement with CardioNet, a wireless cardiac monitoring service provider, arose from a breach
 - Resolution agreement alleged that CardioNet had not fully implemented its HIPAA Security Rule policies and procedures, which were in draft form
 - Is your incident response plan fully approved, adopted and implemented?

Phase 2 HIPAA Audits

- On July 11, 2016, The US Dept. of Health and Human Services Office for Civil Rights (OCR) began a second phase of audits of compliance with the HIPAA privacy, security and breach notification rules
 - As required by the Health Information Technology for Economic and Clinical Health Act
 - 167 covered entities audited
 - Approximately 33 business associates audited
- As expected, the Phase 2 covered entity audits focused on breach notification, as well as security risk analysis and management
- So far, OCR appears to be a tough grader, with many covered entities receiving the lowest scores of 4 or 5 out of 5

Breach Response Lessons Learned From Phase 2 Audits

- OCR appears to be making fine distinctions when determining compliance deficiencies in the Phase 2 audits
- Covered entities have been cited for failure to use breach notification letters that meet all content requirements, including:
 - Recommendations for action the individual can take to protect against harm (such as information about reviewing credit reports)
 - A description of what is being done to investigate the breach
 - What is being done to mitigate harm to the individual
 - Actions to protect against future breaches

Breach Response Lessons Learned From Phase 2 Audits (cont.)

- It's understandable that covered entities will be reluctant to
 - Provide details regarding an investigation
 - Because information can change quickly as the investigation unfolds
 - Provide details regarding mitigation efforts and actions to prevent incident from recurring
 - Being too forthcoming can degrade security
 - Nevertheless, despite this reluctance, make sure that your breach notification letter says something that addresses each of the required informational elements
- Deficiencies cited in Phase 2 audits are likely to reappear in future OCR enforcement actions

OCR's Cyberattack Response Checklist

- This month OCR released a Quick-Response Checklist for cyberattacks
- The guidance is high-level and not particularly surprising
- OCR states that entities experiencing a cyberattack “should” report the crime to law enforcement agencies, which may include
 - State or local law enforcement
 - FBI
 - Secret Services
- However, decision to report to law enforcement is not always so clear-cut
 - Will law enforcement draw additional public attention to incident?
 - Is a particular law enforcement agency likely to vigorously pursue your type of cyberattack?

OCR's Cyberattack Response Checklist

- Cyberattack checklist also states that entities should report all “cyber threat indicators” to federal and information-sharing and analysis organizations (ISAOs), including
 - Dept. of Homeland Security
 - HHS Assistant Secretary for Preparedness and Response
- Reports should not include PHI
- OCR considers all mitigation efforts taken by an entity in any breach investigation, including voluntary sharing of breach-related information with law enforcement agencies and ISAOs
- Not all HIPAA breaches involve “cyber threat indicators” under the Cybersecurity Information Sharing Act of 2015

OCR's Ransomware Guidance

- In a ransomware attack, an intruder deposits malicious software onto a computer system that encrypts data on the victim's network, making it inaccessible to all but the intruder
 - Intruder demands that the system owner pay for an electronic key to unlock the data
- July 11, 2016: OCR issues ransomware guidance that clarifies relationship to the HIPAA Breach Notification Rule
 - When health data is made inaccessible, a breach is deemed to have occurred because an unauthorized party has taken control of the data
 - However, if a health care organization has encrypted its data so that it is unreadable to the intruder, then a breach has not occurred
 - Unless covered entity or business associate can demonstrate that there is a "low probability that the PHI has been compromised," breach is presumed
 - Presence of ransomware will always be a "security incident" under the HIPAA Security Rule

Risk Assessment of Ransomware Infection

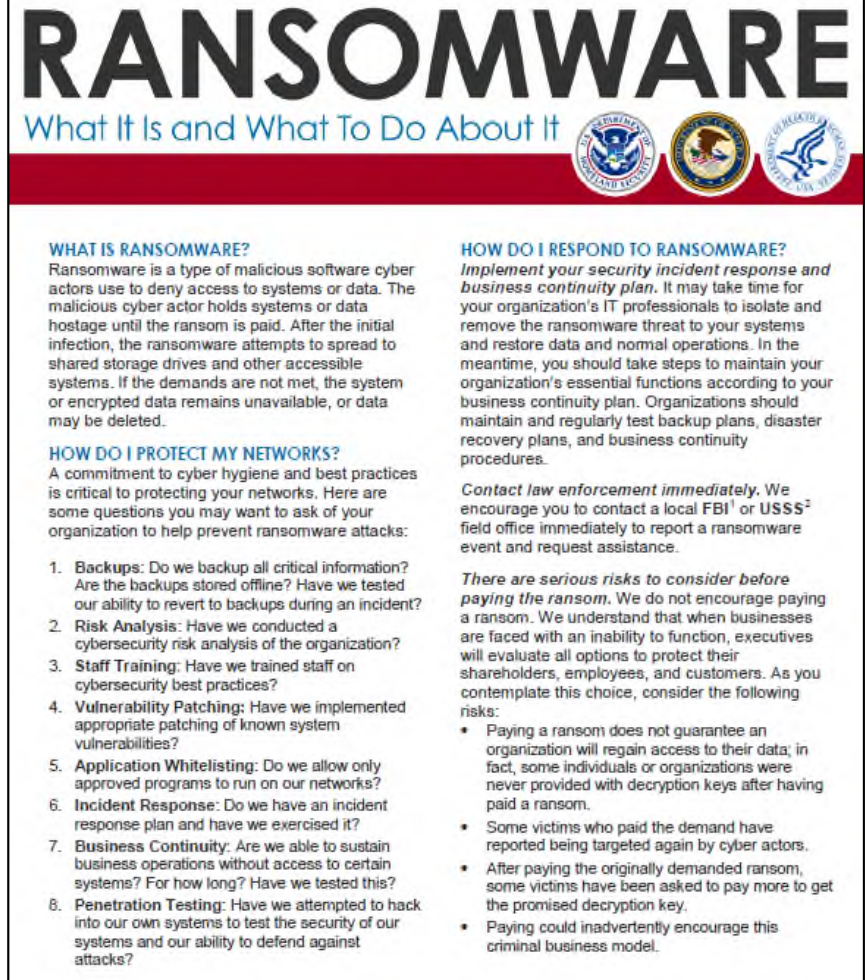
- Analysis of evidence collected through incident response activities can aid in a risk assessment of a ransomware infection, such as:
 - The exact type and variant of the malware discovered
 - The algorithmic steps undertaken by the malware
 - Communications, including exfiltration attempts between the malware and the attackers' command and control servers
 - Whether or not the malware propagated to other systems, potentially affecting other sources of ePHI
- Correctly identifying the malware involved is crucial to understanding its function
- June 2017: HHS disclosed in an email to health care executives and officials that two large, multi-state hospital operators “face significant challenges to operations” from the WannaCry ransomware assault

CYBERSECURITY TRENDS AND ISSUES

RANSOMWARE WHEN A DATA BREACH OCCURS

What Is Ransomware?

- “Ransomware is a type of malicious software cyber actors use to deny access to systems or data.
- “The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems.
- “If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.”



RANSOMWARE

What It Is and What To Do About It

WHAT IS RANSOMWARE?
Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

HOW DO I PROTECT MY NETWORKS?
A commitment to cyber hygiene and best practices is critical to protecting your networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

1. **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training:** Have we trained staff on cybersecurity best practices?
4. **Vulnerability Patching:** Have we implemented appropriate patching of known system vulnerabilities?
5. **Application Whitelisting:** Do we allow only approved programs to run on our networks?
6. **Incident Response:** Do we have an incident response plan and have we exercised it?
7. **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

HOW DO I RESPOND TO RANSOMWARE?
Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove the ransomware threat to your systems and restore data and normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact law enforcement immediately. We encourage you to contact a local FBI¹ or USSS² field office immediately to report a ransomware event and request assistance.

There are serious risks to consider before paying the ransom. We do not encourage paying a ransom. We understand that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

Scope

- “Ransomware is the fastest growing malware threat, targeting users of all types—from the home user to the corporate network.
- “On average, **more than 4,000 ransomware attacks have occurred daily** since January 1, 2016.
- “This is a **300-percent increase** over the approximately 1,000 attacks per day seen in 2015. ”

RANSOMWARE

What It Is and What To Do About It



WHAT IS RANSOMWARE?

Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

HOW DO I PROTECT MY NETWORKS?

A commitment to cyber hygiene and best practices is critical to protecting your networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

1. **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training:** Have we trained staff on cybersecurity best practices?
4. **Vulnerability Patching:** Have we implemented appropriate patching of known system vulnerabilities?
5. **Application Whitelisting:** Do we allow only approved programs to run on our networks?
6. **Incident Response:** Do we have an incident response plan and have we exercised it?
7. **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

HOW DO I RESPOND TO RANSOMWARE?

Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove the ransomware threat to your systems and restore data and normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact law enforcement immediately. We encourage you to contact a local FBI¹ or USSS² field office immediately to report a ransomware event and request assistance.

There are serious risks to consider before paying the ransom. We do not encourage paying a ransom. We understand that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

Payments Increasing

The screenshot shows a CNET news article. At the top left is the CNET logo. To its right are navigation links: REVIEWS, NEWS (highlighted), VIDEO, HOW TO, SMART HOME, CARS, DEALS, and DOWNLOAD. The main headline reads "South Korean web host pays largest ransomware demand ever". Below the headline is a sub-headline: "WannaCry only demanded \$300 from each victim. These hackers extorted \$1 million from one South Korean company." The article is categorized under "Security" and is by Alfred Ng, dated June 20, 2017. There are social media share buttons for Facebook, Twitter, and Email. On the right side of the article, there is a large image showing a person's silhouette in profile, looking at a computer screen. The screen displays a ransomware message with the text "CERBER RANSOMWARE" and some instructions in Korean. The date "June 20, 2017" is written in red at the bottom left of the screenshot area.

South Korean web host pays largest ransomware demand ever

WannaCry only demanded \$300 from each victim. These hackers extorted \$1 million from one South Korean company.

Security

by Alfred Ng
June 20, 2017 10:20 AM PDT
@alfredwing

June 20, 2017

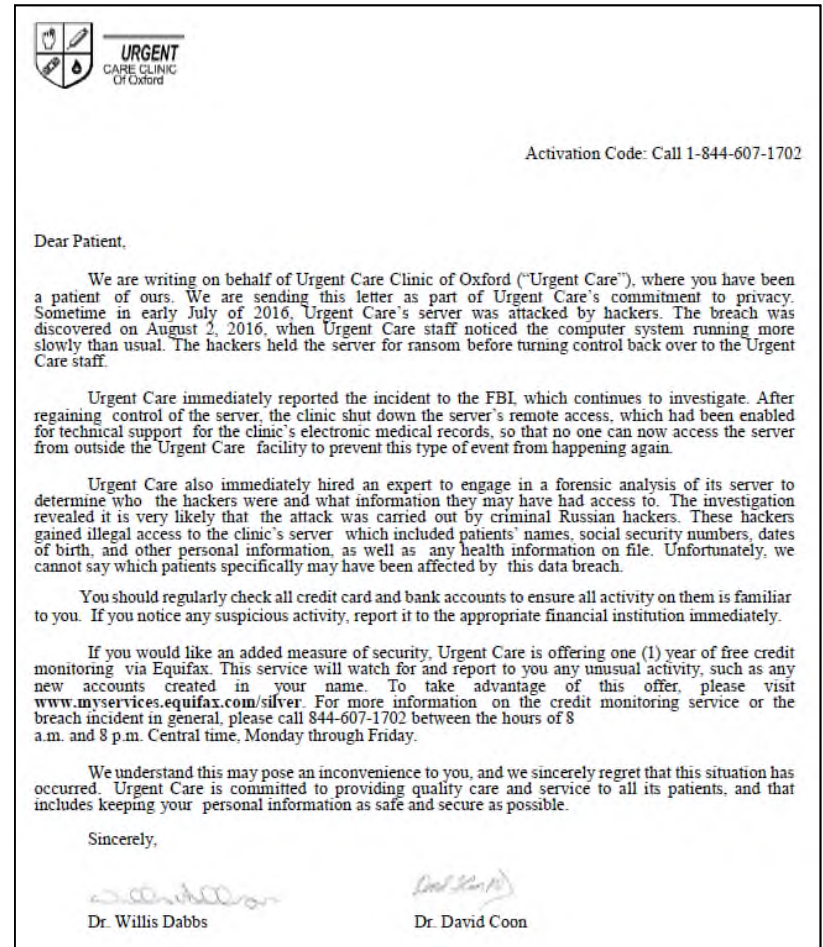
Cerber Ransomware

CERBER RANSOMWARE

...not you find the files you need?
...the content of the files that you looked for not readable?
...is normal because the files' names, as well as the data in your files have been encrypted.
Great!!
You've turned to be a part of a big community #Cerber_Ransomware

Urgent Care Clinic of Oxford (July 2016)

- "Sometime in early July of 2016, Urgent Care's server was attacked by hackers. The breach was discovered on August 2, 2016, when Urgent Care staff noticed the computer system running more slowly than usual. The hackers held the server for ransom before turning control back over to the Urgent Care staff."



Second Ransomware Demand

- Hackers “locked up the files, refusing to give back access unless the hospital paid up.”
- "I'm not at liberty because it's an ongoing investigation, to say the actual exact amount. A small amount was made," the hospital president said.
- After payment, “the hackers didn't return full access to the files” and “**demanded another ransom.**”
- “The hospital says, it will not pay again.”



The image is a screenshot of a news article from KWCH12. The header features the station's logo "KWCH12 expect more" and navigation links for Weather, Sports, Station Info, Catch It Kansas, and Livestream. The article title is "Hackers demand ransom payment from Kansas Heart Hospital for files". Below the title is a video player showing the exterior of the Kansas Heart Hospital building. The article text describes a ransomware attack on the hospital, mentioning that the president, Dr. Greg Duick, says the hackers never got access to patient information. It also notes that this is a common type of attack, with 45% of hospitals having received some kind of cyber attack. The article includes social media sharing icons and a timestamp of 10:01:67°.

KWCH12
expect more

Home / Crime / Article

Hackers demand ransom payment from Kansas Heart Hospital for files

By Deedee Sun | Posted: Fri 10:34 PM, May 20, 2016 | Updated: Fri 10:37 PM, May 20, 2016

WICHITA, Kan. A hospital held hostage by hackers and denied access to its files until it pays a ransom. It's a crime that's been reported across the country, and now it's happened in Wichita.

It's called "ransomware" - hackers hijack your computer and hold the data until you pay up.

The Kansas Heart Hospital is the latest victim of this attack.

The hospital's president, Dr. Greg Duick, says the hackers never got access to patient information, but the attack did cause problems.

"Kansas Heart Hospital had a cyber attack occur late Wednesday evening," Duick said. "We suspect, as attacks other parts of the country, this was an offshore operation," he said.

Duick says hackers holding hospital files hostage is very common.

"Upwards of 45% of hospitals have received some kind of cyber attack. And multiple hospitals had additional attacks," he said.

About 9pm Wednesday, a hospital employee lost access to files.

Payment?

"We do not encourage paying a ransom.

As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model."

RANSOMWARE

What It Is and What To Do About It



WHAT IS RANSOMWARE?

Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

HOW DO I PROTECT MY NETWORKS?

A commitment to cyber hygiene and best practices is critical to protecting your networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

1. **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training:** Have we trained staff on cybersecurity best practices?
4. **Vulnerability Patching:** Have we implemented appropriate patching of known system vulnerabilities?
5. **Application Whitelisting:** Do we allow only approved programs to run on our networks?
6. **Incident Response:** Do we have an incident response plan and have we exercised it?
7. **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

HOW DO I RESPOND TO RANSOMWARE?

Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove the ransomware threat to your systems and restore data and normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact law enforcement immediately. We encourage you to contact a local FBI¹ or USSS² field office immediately to report a ransomware event and request assistance.

There are serious risks to consider before paying the ransom. We do not encourage paying a ransom. We understand that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

Statement on reported NHS cyber attack

A number of NHS organisations have reported to NHS Digital that they have been affected by a ransomware attack.

The investigation is at an early stage but we believe the malware variant is Wanna Decryptor.

This attack was not specifically targeted at the NHS and is affecting organisations from across a range of sectors.

At this stage we do not have any evidence that patient data has been accessed.

NHS Digital is working closely with the National Cyber Security Centre, the Department of Health and NHS England to support affected organisations and ensure patient safety is protected.

Our focus is on supporting organisations to manage the incident swiftly and decisively, but we will continue to communicate with NHS colleagues and will share more information as it becomes available.

Notes to editors

As at 15.30, 16 NHS organisations had reported that they were affected by this issue.

Recent Ransomware Example



13 May 2017

Alert Number
MC-000081-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact FBI CYWATCH immediately.

Email:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

Indicators Associated With WannaCry Ransomware

This is a joint product with the Department of Homeland Security.

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP: WHITE**: This information may be distributed without restriction.

Summary

According to numerous open-source reports, a widespread ransomware campaign is affecting various organizations with reports of tens of thousands of infections in as many as 99 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The software can run in as many as 27 different languages. The latest version of this ransomware variant, known as WannaCry, WCry, or Wanna Decryptor, was discovered the morning of May 12, 2017, by an independent security researcher and has spread rapidly over several hours, with initial reports beginning around 4:00 AM EDT, May 12, 2017. Open-source reporting indicates a requested ransom of .1781 bitcoins, roughly \$300 U.S.

Ransomware Protection and Issues

Protection and Prevention

- Offline and Secure Backups
- Avoiding Links or Phishing Schemes with Attachments Containing Malware
- Strong Passwords
- Update Operating Systems, Software, and Patches and Use Antivirus Software
- Monitoring and Intrusion Detection
- Tailored Protections
- Incident Response Plan That Is Tested

Ransomware Protection and Issues

Legal Issues

- Initial Cyber Investigation under Attorney-Client Privilege
- Determining Any Notification Requirements
- Response to Government Inquiries and Enforcement Actions
- Anticipating Potential Civil Litigation
- Contacting Law Enforcement
- Information Sharing in the Private and Public Sectors
- Scope of Cyber-Insurance Coverage

Takeaways

- Security breaches pose the single greatest privacy and security regulatory risk for healthcare organizations
 - Often leads to OCR investigations, particularly larger breaches
 - Prompts OCR to examine an organization's overall security compliance program
- A HIPAA security breach is not necessarily a violation of HIPAA standards – current cyber threats are sophisticated and no organization is immune
- Failure to implement an appropriate security incident response plan IS a HIPAA violation
- A thoughtful, documented, battle-tested incident response plan is the best way to mitigate reputational harm and defuse regulatory scrutiny related to a breach

Thanks!



Reece Hirsch

Partner

Morgan Lewis

+1.415.442.1422

reece.hirsch@morganlewis.com



Mark Krotoski

Partner

Morgan Lewis

+1.650.843.7212

mark.krotoski@morganlewis.com



Jake Harper

Associate

Morgan Lewis

+1.202.739.5260

jacob.harper@morganlewis.com

Join us next month!

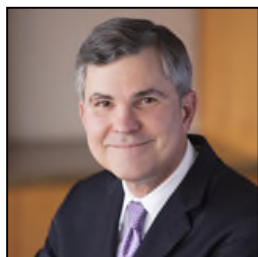
Please join us for next month's webinar:

["New Considerations in Negotiating CIAs"](#)

Featuring Scott Memmott and Holly Barker

➤ July 27, 2017 3:00 PM (EST)

Mark Krotoski



Partner

Office: San Francisco

Email: reece.hirsch@morganlewis.com

Phone: +1.415.442.1422

[Click here for full bio](#)

- W. Reece Hirsch counsels clients on healthcare regulatory and transactional matters and co-heads the firm's privacy and cybersecurity practice.
- Reece represents healthcare organizations such as hospitals, health plans, insurers, physician organizations, healthcare information technology companies, and pharmaceutical and biotech companies,
- He advises clients on issues such as privacy, fraud and abuse, and self-referral issues. This includes healthcare-specific data privacy and security matters, such as compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act.

Mark Krotoski



Partner

Office: Silicon Valley

Email: mark.krotoski@morganlewis.com

Phone: +1.650.843.7212

[Click here for full bio](#)

- Litigation partner in the Privacy and Cybersecurity and Antitrust practices.
- 20 years' experience handling cybersecurity cases and issues, he advises clients on mitigating and addressing cyber risks, developing cybersecurity protection plans, responding to a data breach or misappropriation of trade secrets, conducting confidential cybersecurity investigations, and coordinating with law enforcement on cybercrime issues where appropriate.
- Handles a variety of complex and novel investigations and high-profile cases and has led prosecutions and investigations of nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, and criminal intellectual property cases.
- Served as the national coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, in addition to other DOJ leadership positions.