The Cyber Threat Landscape for Healthcare Providers: Protecting Electronic Systems and Lifesaving Equipment

Dawn C. Bruno, *Supervisory Special Agent and Associate Division Counsel, FBI*

Lani M. Dornfeld, Esq., *Brach Eichler LLC*

Riza I. Dagli, **Esq.,** *Brach Eichler LLC*

Cyber/Phishing Incident

- Employee received email from what looked like one of the facility's contacts.
- Email content looked legitimate, except something seemed "off" about the grammar, punctuation, and style of writing.
- Employee nonetheless clicked on a link in the email.
- Employee's computer started "acting funny," and she called the IT manager.

- IT manager discovered that clicking on the link introduced a destructive malware software into the organization's systems.

Social Media Incident

- Medical practice receptionist took a photo on her cell phone of artwork her child made at school, that was hanging on the corner of her computer monitor.
- She posted the photo on her social media account.
- The photo depicted not only the child's artwork but also the patient scheduler that was on her computer screen.
- One day later, practice received call from someone in the community, advising of the "breach of patient information."

- The patient schedule shown in the photograph included patient names, date and time of appointment, scheduled medical service, patient telephone number, and other protected health information.

Insider Threats

- Employee of healthcare provider gave 2 weeks' notice on Friday.
- HR and IT are notified, to schedule return of employer-owned property and to coordinate system access termination on the scheduled termination date.
- On Monday, employee came to work and said, "You guys owe me back pay and I am out of here." HR is notified, but through an oversight IT is not notified.
- The employee went home, and over the next 2 weeks, accessed the employer's systems multiple times, including emails and PHI.

- The employee then filed a written complaint with the OCR, stating the employer impermissibly allowed the employee to have continued access after termination.

BRACH EICHLER LLC
Counsellors at Law

NJHMR
HEALTHCARE MARKET REVIEW

Email Hacking Incident

- CFO of large, multi-office medical practice received an email that purported to be from the CEO of the practice. Attached to the email was an invoice, and in the body of the email, the "CEO" advised that the invoice was overdue and must be paid immediately. The invoice amount was over $100,000 and was from a company in Hong Kong.

- Nothing in the email itself raised suspicion, since the email looked like it legitimately came from the CEO. Nonetheless, the invoice raised the suspicion of the CFO, who then called the CEO to ask about the email. The CEO said he did not send it.

- IT researched the incident and discovered that the email system had been "hacked" by outsiders.

Ransomware Incident

- On Sunday night, the IT manager noticed some “suspicious activity” on the ASC’s systems. He emailed the administrator.
- On Monday morning, staff was unable to access certain computer systems at the center.
- When the administrator opened her email that morning, she received an email message stating the system has been locked and asking for bitcoin ransom in return for the decryption key.
- The affected systems included the demographic/billing software system and certain files stored on the server. At first glance, it did not appear that the EMR was locked.

Federal Bureau of Investigation

Roles and Responsibilities for Federal Cybersecurity are aligned with those of DHS and DoD

Regarding cyber threats:

- The FBI and DOJ assume the lead for **investigation** and **enforcement.**
- DHS is charged with **protection** and the DoD with **national defense**.
- DHS works with state, local, tribal, territorial (SLTT) agencies, and private sector companies to prioritize cyber recovery efforts for critical systems.
- DHS also leads the defense of the .gov network.
- The FBI routinely coordinates with the U.S. Secret Service, particularly their domestic and international Electronic Crimes Task Forces on cyber issues.
- DoD leads the defense of the .mil network.

Constant coordination with our public, private, and international partners is paramount to our nation's cybersecurity.

Federal Bureau of Investigation Director Wray

- Worried about a wider-than-ever range of threat actors.
- Concerned about a wider-than-ever gamut of methods, from botnets to ransomware, and from spear phishing to business email compromise.
- Seeing these diverse threats in almost every company, at almost every level.
- The days of wondering if you're going to be the next victim are gone. Instead, it's a matter of when, or even how often you'll get hit, and how bad it'll be when it happens.
- Every company – every bank, every firm – every agency is a target.
- Every single bit of information, every system, every network is a target.
- Every link in the chain is a potential vulnerability. Even your own employees and contractors – what we call the insider threat.

4 in 5

U.S. physicians have experienced some form of a cybersecurity attack

$408

per record cost of a data breach in 2018

***health care has highest cost across all industries**

$2.2 million

average cost of a data breach for health care organizations

https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

$6.2 billion lost by U.S.

Health Care System in 2016 due to data breaches

https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

BRACH | EICHLER LLC
Counsellors at Law

NJ HMR
HEALTHCARE MARKET REVIEW

Cyber Threat Actors Broadly

The FBI has the statutory authority to investigate crimes associated with below

- ***Hacktivist*:** Redress perceived wrong/advance malicious agenda - defacements, DDoS, exfiltration, destructive malware
- ***Financially Motivated Actor*:** intrusions/hacking using Ransomware, Business E-mail Compromise
- ***Insider Threat Actor*:** Witting or Accidental – all employees with access to sensitive data, 3rd party contractors and partners, IT administrators.
- ***Nation State (Espionage, Warfare)*:** Military/economic advantage - Advanced Persistent Threats (APTs) - seek sensitive state secrets, proprietary information from companies using a wide range of techniques; sabotage military and critical infrastructure systems. Both DOD and FBI statutory authority.
- ***Cyber Terrorist*:** Sabotage/terror – e.g., computer systems that operate critical infrastructure

Multiple/combination motivations

Common Methods and Vulnerabilities

- ***Phishing*** - when an adversary conceals a link or file containing malware in something like an email, text message, or social media message that looks like it is from a legitimate organization or person (spoofing). If clicked, malware in the link or file compromises the recipient's electronic device and/or associated account and can provide criminals with full control of the user's computer, including access to passwords, documents, and e-mail.

ceo@abc-company.com

ceo@abc_company.com

jane.smith@abccompany.com

jane-smith@abccompany.com

jane.smith@abccompany1.com [number 1]

jane.smith@abccompanyl.com [lower case l]

Common Methods and Vulnerabilities (cont.)

- ***Business E-Mail Compromise*** - a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests. The scam is frequently carried out when a subject compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds. The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information or Wage and Tax Statement (W-2) forms.

  Post cyber intrusion, sophisticated cyber criminals may even monitor business communications for extended periods of time in order to understand operating procedures and the communication style of the individuals they want to impersonate.

Between October 2013 and July 2019,
FBI identified 166,349 domestic and international incidents with over $26 billion in losses
Between May 2018 and July 2019 - 100 percent prior term increase in identified global exposed losses
$676m-$1.3b

Common Methods and Vulnerabilities (cont.)

- ***Social Engineering*** – adversary tricks a user into divulging confidential or personal information that may be used for fraudulent purposes or gains the info from a variety of open sources (profiles, content, and interactions on social media websites) as well as other intrusions to spot and assess employees for exploitation of their access.
- ***Unpatched Software Exploration*** – adversary takes advantage of people or companies that do not update their software regularly and conduct malicious activity such as computer exploitation or malware installation.

Common Methods and Vulnerabilities (cont.)

- ***Ransomware*** - a form of malware that after infecting a computer or network, typically denies the user access to their data or systems until a sum of money is paid. Typical infection methods include clicking on malicious phishing e-mail links, visiting infected websites, and the exploitation of weak Remote Desktop Protocol (RDP) passwords.

  Usually, all files are encrypted and effectively locked away from the user. The criminal notifies the victim that they must pay a ransom in order to receive a digital key to unlock and retrieve their files.

  Recent ransomware campaigns have employed a robust encryption that prevents most attempts to break the encryption and recover the data.

  The key areas to focus on with ransomware are prevention, business continuity, and remediation. Secure your backups! Ensure backups are not connected to the computers and networks they are backing up.

Common Methods and Vulnerabilities (cont.)

Internet of Things (IOT) – Director Wray's Speech – "Every single bit of information, every system, every network is a target. Every link in the chain is a potential vulnerability."

Internet-connected medical devices – unchangeable administrative passwords; access to electronic medical record systems; outdated software with no compatibility between legacy operating systems; adding encryption to implanted medical devices would require a more powerful processor – substantially reduce battery life.

Health information technology, which provides critical life-saving functions, consists of connected, networked systems and leverages wireless technologies, leaving such systems more vulnerable to cyber-attack.

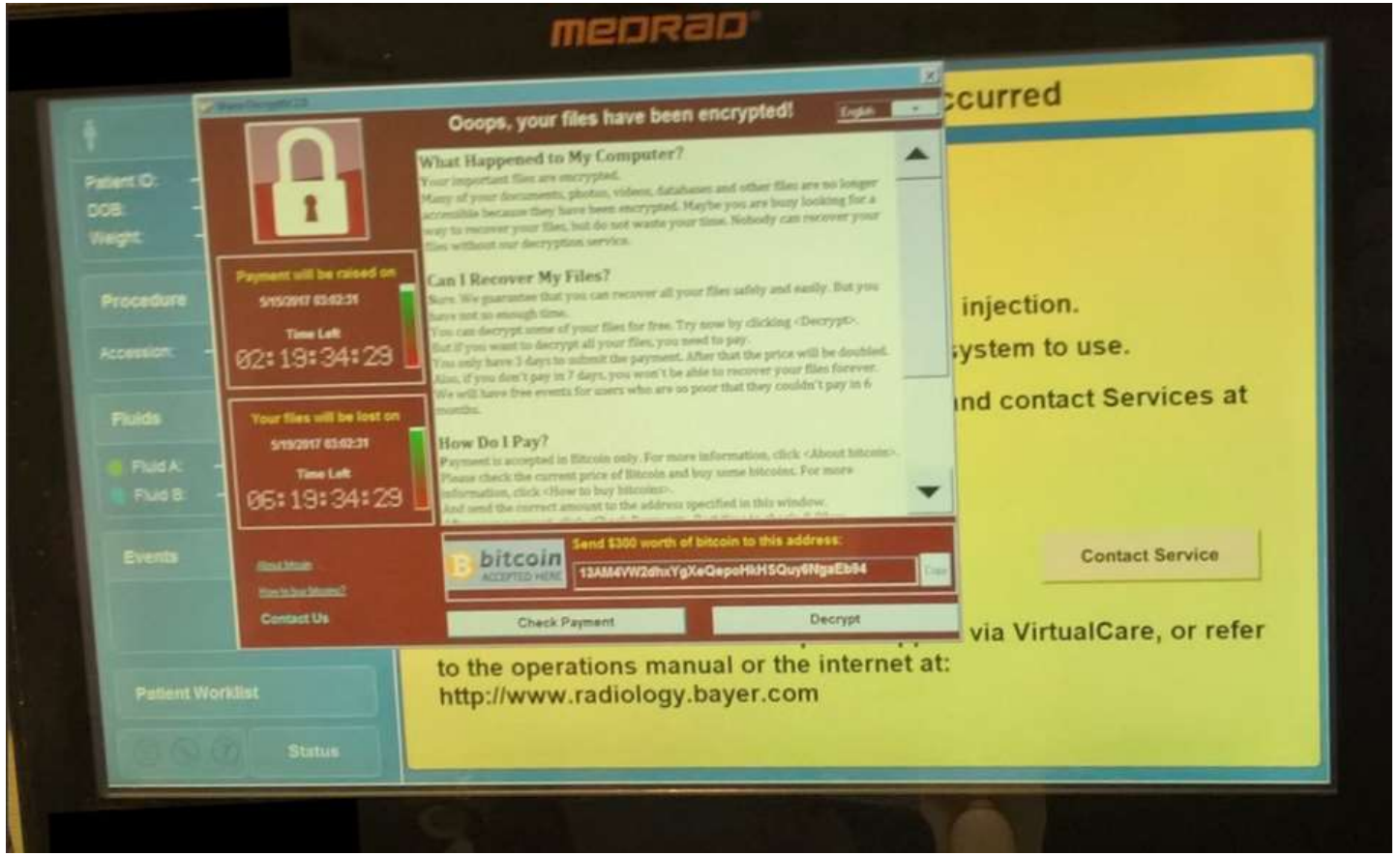
HHS-Identified Vulnerabilities
MEDICAL EQUIPMENT

- Patches not implemented promptly; includes regular and routine commercial system patches to maintain medical devices.
- Equipment not current, or legacy equipment that is outdated and lacks current functionality.
- Most medical devices, unlike IT equipment, cannot be monitored by an organization's intrusion detection system (IDS); safety of patients and protection of data integrity are dependent on identifying and understanding the threats and threat scenarios – the challenge of identifying and addressing vulnerabilities in medical devices that augments the risk of threats compared with managed IT products.
- For medical devices, the cybersecurity profile information is not readily available at health care organizations, making cybersecurity optimization more challenging. This may translate into missed opportunities to identify and address vulnerabilities, increasing the likelihood for threats to result in adverse effects.
- Heterogeneity of medical devices means that the vulnerability identification and remediation process is complex and resource intensive; increases the likelihood that devices will not be assessed or patched, leading to missed opportunities to close vulnerabilities.

May 2017 *Forbes* Article

Medical Devices Hit By Ransomware For The First Time In US Hospitals

Thomas Brewster Forbes Staff
Cybersecurity
I cover crime, privacy and security in digital and physical forms.



BRACH EICHLER LLC
Counsellors at Law

NJHMR
HEALTHCARE MARKET REVIEW

HHS 2018 OIG Report

"In addition to issuing guidance, FDA continues to address myths about medical device cybersecurity and published a fact sheet entitled 'The FDA's Role in Medical Device Cybersecurity, Dispelling Myths and Understanding Facts.' In the fact sheet, FDA clarified it is a myth that '[t]he FDA tests medical devices for cybersecurity.' It is fact that '[t]he FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer.' FDA's fact sheet also states it is myth that '[t]he FDA is responsible for the validation of software changes made to address cybersecurity vulnerabilities.' It is fact that '[t]he medical device manufacturer is responsible for the validation of all software design changes, including computer software changes to address cybersecurity vulnerabilities.'"

Be Proactive: Hand Hygiene for Cybersecurity

Just as healthcare professionals must wash their hands before caring for patients, health care organizations must practice good “cyber hygiene” in today’s digital world, including it as a part of daily universal precautions. Like the simple act of hand-washing, a culture of cyber-awareness does not have to be complicated or expensive for a small organization. It must simply be effective at enabling organization members to protect information that is critical to the organization’s patients and operations.

- Scrutinize addresses and links contained in e-mails; do not open attachments or click on pictures in unsolicited e-mails.
- Disable macros. Be careful of pop-ups from attachments that require users to enable them.
- Only download software–especially free software–from known and trusted sites.
- Do not use the same login and password for multiple platforms, servers, or networks.

Proactive Steps

Consult the **National Institute of Standards and Technology (NIST) Cybersecurity Framework.** The framework presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization. The framework consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover.

- The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities.
- The Protect Function outlines appropriate safeguards to ensure delivery of critical services.
- The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event
- The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident.
- The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

See HHS site for NIST model for HealthCare industry: https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

BRACH EICHLER LLC
Counsellors at Law

NJHMR
HEALTHCARE MARKET REVIEW

Proactive Steps (cont.)

There are steps organizations may take to identify and deter potential cyber intrusions. The FBI offers these for information, but each company must assess applicability in terms of its own policies, processes, and legal guidelines.

- Know your network and what attaches to it.
- Educate and regularly train employees on security policies and protocols.
- Update software, firewalls, and anti-virus programs.
- Install Intrusion Detection Systems (IDSs).
- Establish Virtual Private Networks (VPNs) for added protection.
- Ensure proprietary information online is carefully protected.
- Employ appropriate screening processes to hire new employees.
- Provide nonthreatening, convenient methods for employees to report .suspicious behavior, and encourage such reporting.
- Routinely monitor computer networks for suspicious activities.
- Ensure physical security personnel and information technology security personnel have the tools they need to share information.
- Encourage responsible use of social media sites and ensure online profiles have proper security protections in place.

Proactive Steps/Resources

- The FBI leads and encourages participation in the Cyber Health Working Group through the **InfraGard Program**, which encourages IT professionals in the healthcare industry to share real-time tactical information about threats, trends, and best practices.
- The **Domestic Security Alliance Council** (DSAC) is a strategic partnership between the U.S. government and the U.S. private industry that enhances communication and promotes the timely and effective exchange of security and intelligence information between the federal government and the private sector.
- The FDA provides pre and post-market guidance for the management of cybersecurity in medical devices.
- The Department of Homeland Security (DHS), US-CERT, and the Department of Health and Human Services provide additional resources for government and industry cybersecurity support. Information is available on their respective Web sites.

https://www.us-cert.gov/resources

includes company self-assessment and other valuable resources

https://search.us-cert.gov/search

search by term – e.g., “medical” for advisories and alerts

https://www.cisa.gov

Cybersecurity and Infrastructure Security Agency (CISA)

https://www.dhs.gov/topic/cybersecurity#

ICS Medical Advisory (ICSMA-19-029-01)
Stryker Medical Beds
Original release date: January 29, 2019

Successful exploitation of this vulnerability could allow data traffic manipulation, resulting in partial disclosure of encrypted communicatio... An industry-wide vulnerability exists in the WPA and WPA2 protocol affected by the Key Reinstalla... KRACK. The four-way hand shake traffic in the Wi-Fi Protected Access WPA and W... nonce reuse, resulting in key reinstallation. This could allow an ... attacker within radio range to replay, ...

"The KRACK vulnerability is applicable to iBed Wireless-enabled Secure II, S3 and InTouch beds that are wirelessly-connected to a hospital network." -https://www.stryker.com, May 2019

NCCIC recommends users take defensive measures to ...
Specifically, users should:

•Minimize network exposure for all control system devices and/or systems, and ensure that they ... accessible from the Internet.

•Locate control system networks and remote devices behind firewalls, and isolate them from the business network.

•When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

NCCIC reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

https://www.us-cert.gov/ics/advisories/ICSMA-19-029-01

Cyber Incident Reporting

If you are the victim of a serious cyber incident, HHS recommends the following steps:

- Contact your FBI Field Office Cyber Task Force www.fbi.gov/contact-us/field/field-offices immediately to report a cyber incident and request assistance. The FBI works with state and local law enforcement and other federal and international partners to pursue cyber criminals globally and to assist victims of cyber-crime.

- Report cyber incidents to the US-CERTwww.us-cert.gov/ncas and FBI's Internet Crime Complaint Center www.ic3.gov

Investigation of Cyber or Other Breach Incident: Swift Action a Must

- **Assemble a response team immediately**
  - HIPAA Privacy Officer
  - HIPAA Security Officer
  - IT Manager?
  - HR Manager?
  - Compliance Officer/Committee?
  - Need forensic IT or cyber response experts?
  - Should legal counsel be consulted? (attorney-client privilege)
  - Does leadership need to be notified?
  - Need public relations professionals?

Mitigation

- As early in the investigative process as possible, the covered entity should seek to take mitigating actions to contain the breach or prevent additional or future similar breaches

- Mitigating actions will assist in risk assessment and help reduce liability

Investigation: Careful, Planned Approach

Investigative steps flow from breadth and type of incident

IT incidents

- Website breach (“contact us” or payment portal)
- Patient portal breach
- Phishing, malware, hacking, ransomware or similar cyber incident
- PHI becomes publicly-facing on the internet
- Loss/theft of computer or other electronic device
- Unauthorized access to systems

Impermissible disclosure incidents

- Violation of minimum necessary standard
- Misdirected mail or fax
- Curious staff members
- Sharing of IT credentials
- Allegation of over-disclosure
- Disclosure without or beyond scope of written authorization
- Social media disclosure

Investigation: Who, What, When, Where, Why?

Who…

- Determine relevant individuals to interview; more interviews will likely flow from information received in initial interviews
- Ratio: 2 interviewers to 1 interviewee
- Focus questions on the Who, What, When, Where, and Why of the incident
- Conduct in private; document all interviews in writing
- Advise interviewees to maintain confidentiality of investigation
- Interview results should provide guidance to next steps

Other Investigative Steps

Document Review and Forensic Review

- Determine from interviews and information gathered what further documents and other information needs to be reviewed
  - Review of correspondence, audit logs, emails, social media posts, etc.
- Determine if need IT expert for forensic review
  - Was there human input error, systems error, system flaws or weaknesses, cyber attack, other IT problem?

Guilty Until Proven Innocent

- Must conduct HIPAA risk assessment: any impermissible acquisition, access, use, or disclosure of PHI is *presumed* to be a breach, unless prove otherwise through multi-factor risk assessment
  - Nature and extent of PHI
  - Unauthorized person
  - Actually acquired or viewed
  - Mitigating actions
- If, through risk assessment, can demonstrate there is a “low probability” PHI has been “compromised,” then no mandatory reporting
  - “Compromise” is not defined in the rule

Document, Document, Document…

- Investigative notes, statements, documents, reports, analyses, relevant agreements (e.g., BAAs), audit logs
  - What might OCR ask for if this issue is investigated?
- Investigative summary report
  - Risk assessment

HIPAA Breach Notification

- Need to determine and make required notifications by deadlines:
  - Affected individuals
  - The OCR
  - The media
  - Other agencies?

New Jersey Reporting Obligations

- NJSA 56:8-163 Disclosure of breach of security to customers.
  - Any business that conducts business in New Jersey… shall disclose any breach of security of computerized records following discovery to any customer who is a resident of New Jersey whose personal information was accessed.
  - But, must contact New Jersey State Police first!
- If affected patients reside in other states, need to review each state's identity theft and breach notification laws.

New Jersey Cybersecurity & Communications Integration Cell (NJCCIC)

Data breaches must be reported to the New Jersey State Police through a centralized agency, NJCCIC.
databreach@cyber.nj.gov

- Statutory notification to customers shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation.

Cybercrime Criminal Statutes

- 18 U.S. Code § 1030 Fraud in connection with computers
- 2C:21-17 Impersonation; theft of identity
- 2C:20-25 Computer crimes
- 2C:20-31 Wrongful computer access
- Other related crimes often involved, e.g., extortion and theft.

Why Does This Matter?

Reputational Harm

Financial Loss

Civil Money Penalties
Business Interruption

DHHS “Wall of Shame”

Criminal Penalties

Disclaimer:

This presentation and outline are designed to provide accurate and authoritative information regarding the subject matter covered. This presentation and outline should not be construed as legal advice or as pertaining to specific, factual situations. If legal advice or other expert assistance is required, the services of a competent professional should be sought.