American Hospital Association™

Advancing Health in America

Cyber Security and Risk in the Hospital Space

Presented by John Riggi, AHA Senior Advisor for Cybersecurity and Risk

November 5, 2018

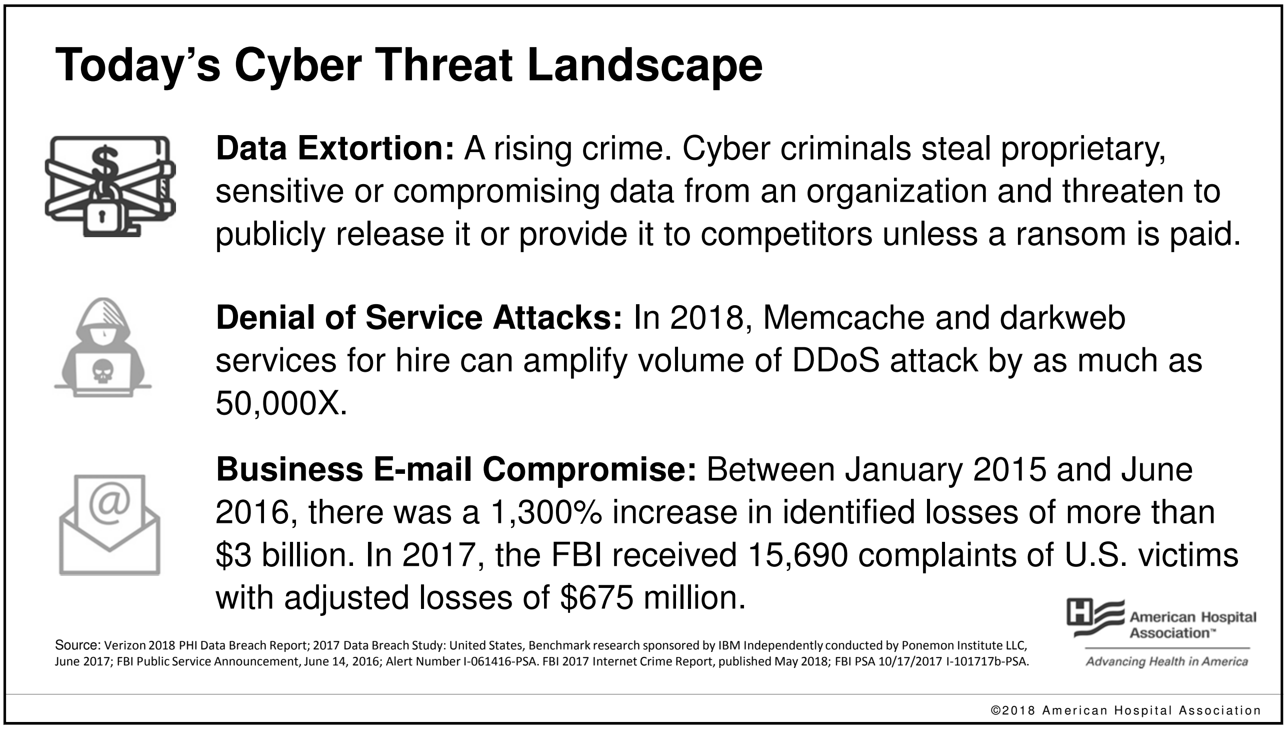
Agenda

- Cyber Threat Landscape and Emerging Threats
- Top 12 Risk Considerations for Leadership
- Additional Topics
  - Medical Devices
  - Cyber Insurance
- Takeaways
- The AHA's Cybersecurity and Risk Advisory Services
- ***Discussion and questions throughout***

American Hospital Association™

Advancing Health in America

The Cyber Threat Landscape



Today's Cyber Threat Landscape

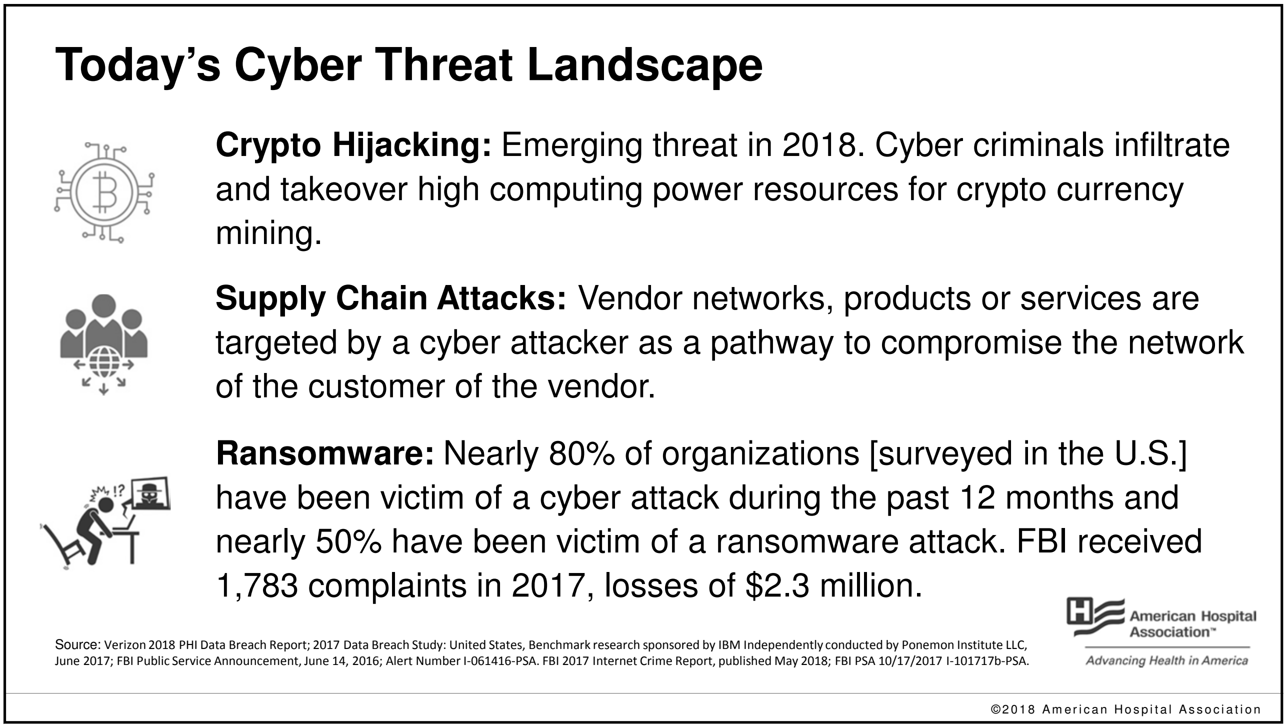
Data Extortion: A rising crime. Cyber criminals steal proprietary, sensitive or compromising data from an organization and threaten to publicly release it or provide it to competitors unless a ransom is paid.

Denial of Service Attacks: In 2018, Memcache and darkweb services for hire can amplify volume of DDoS attack by as much as 50,000X.

Business E-mail Compromise: Between January 2015 and June 2016, there was a 1,300% increase in identified losses of more than $3 billion. In 2017, the FBI received 15,690 complaints of U.S. victims with adjusted losses of $675 million.

Source: Verizon 2018 PHI Data Breach Report; 2017 Data Breach Study: United States, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, June 2017; FBI Public Service Announcement, June 14, 2016; Alert Number I-061416-PSA. FBI 2017 Internet Crime Report, published May 2018; FBI PSA 10/17/2017 I-101717b-PSA.

American Hospital Association™
Advancing Health in America



Today’s Cyber Threat Landscape

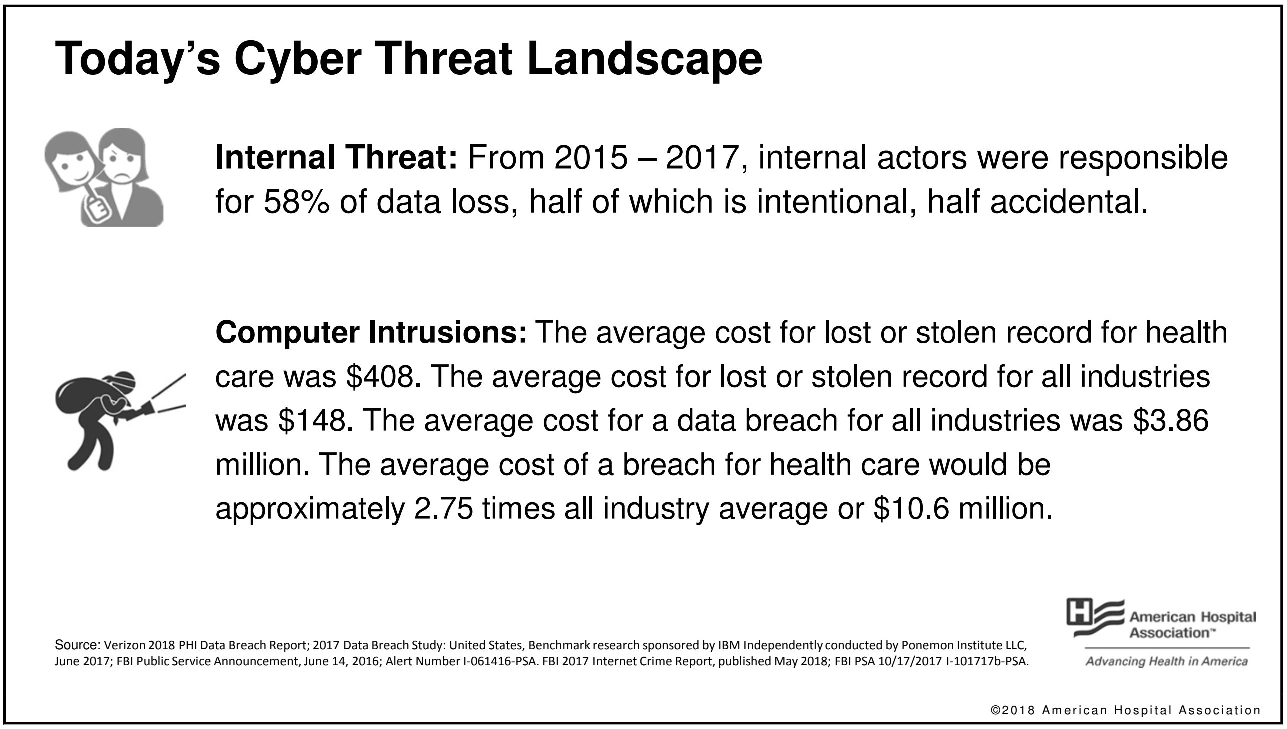
Crypto Hijacking: Emerging threat in 2018. Cyber criminals infiltrate and takeover high computing power resources for crypto currency mining.

Supply Chain Attacks: Vendor networks, products or services are targeted by a cyber attacker as a pathway to compromise the network of the customer of the vendor.

Ransomware: Nearly 80% of organizations [surveyed in the U.S.] have been victim of a cyber attack during the past 12 months and nearly 50% have been victim of a ransomware attack. FBI received 1,783 complaints in 2017, losses of $2.3 million.

Source: Verizon 2018 PHI Data Breach Report; 2017 Data Breach Study: United States, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, June 2017; FBI Public Service Announcement, June 14, 2016; Alert Number I-061416-PSA. FBI 2017 Internet Crime Report, published May 2018; FBI PSA 10/17/2017 I-101717b-PSA.

American Hospital Association™
Advancing Health in America



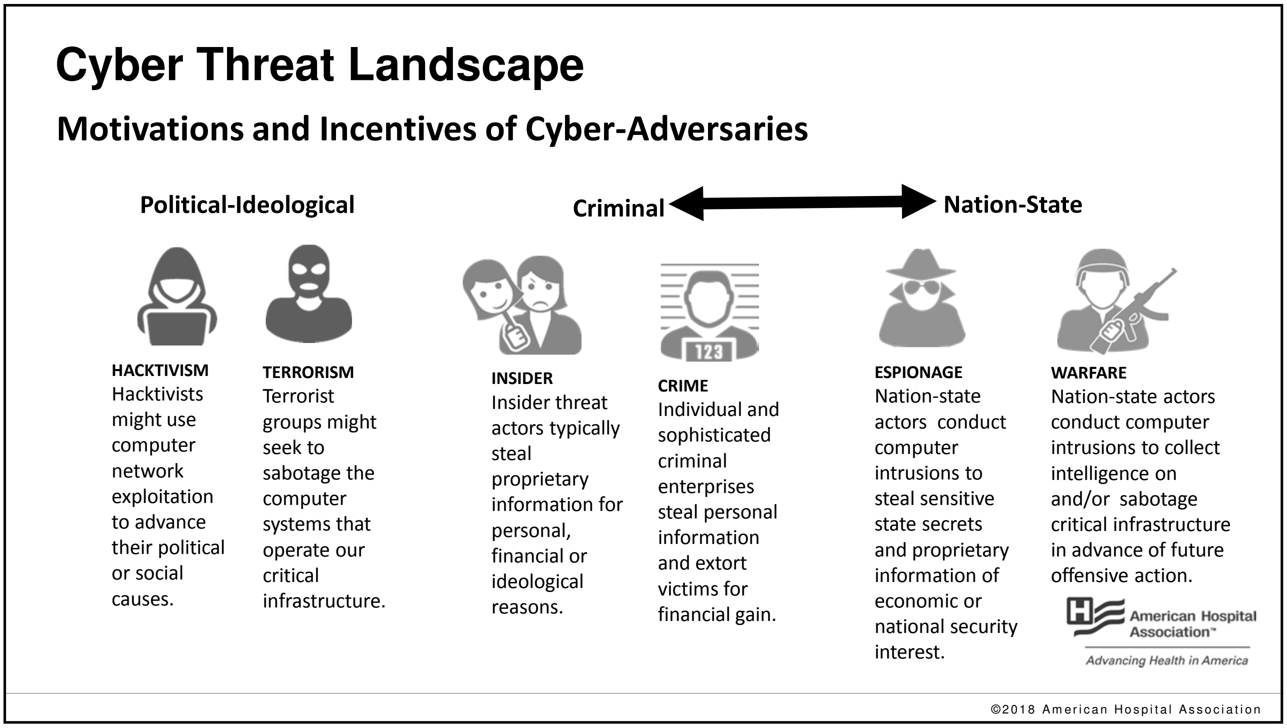
Today’s Cyber Threat Landscape

Internal Threat: From 2015 – 2017, internal actors were responsible for 58% of data loss, half of which is intentional, half accidental.

Computer Intrusions: The average cost for lost or stolen record for health care was $408. The average cost for lost or stolen record for all industries was $148. The average cost for a data breach for all industries was $3.86 million. The average cost of a breach for health care would be approximately 2.75 times all industry average or $10.6 million.

Source: Verizon 2018 PHI Data Breach Report; 2017 Data Breach Study: United States, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, June 2017; FBI Public Service Announcement, June 14, 2016; Alert Number I-061416-PSA. FBI 2017 Internet Crime Report, published May 2018; FBI PSA 10/17/2017 I-101717b-PSA.

American Hospital Association™
Advancing Health in America



Cyber Threat Landscape

Motivations and Incentives of Cyber-Adversaries

Political-Ideological

Criminal ⟷ **Nation-State**

HACKTIVISM
Hacktivists might use computer network exploitation to advance their political or social causes.

TERRORISM
Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.

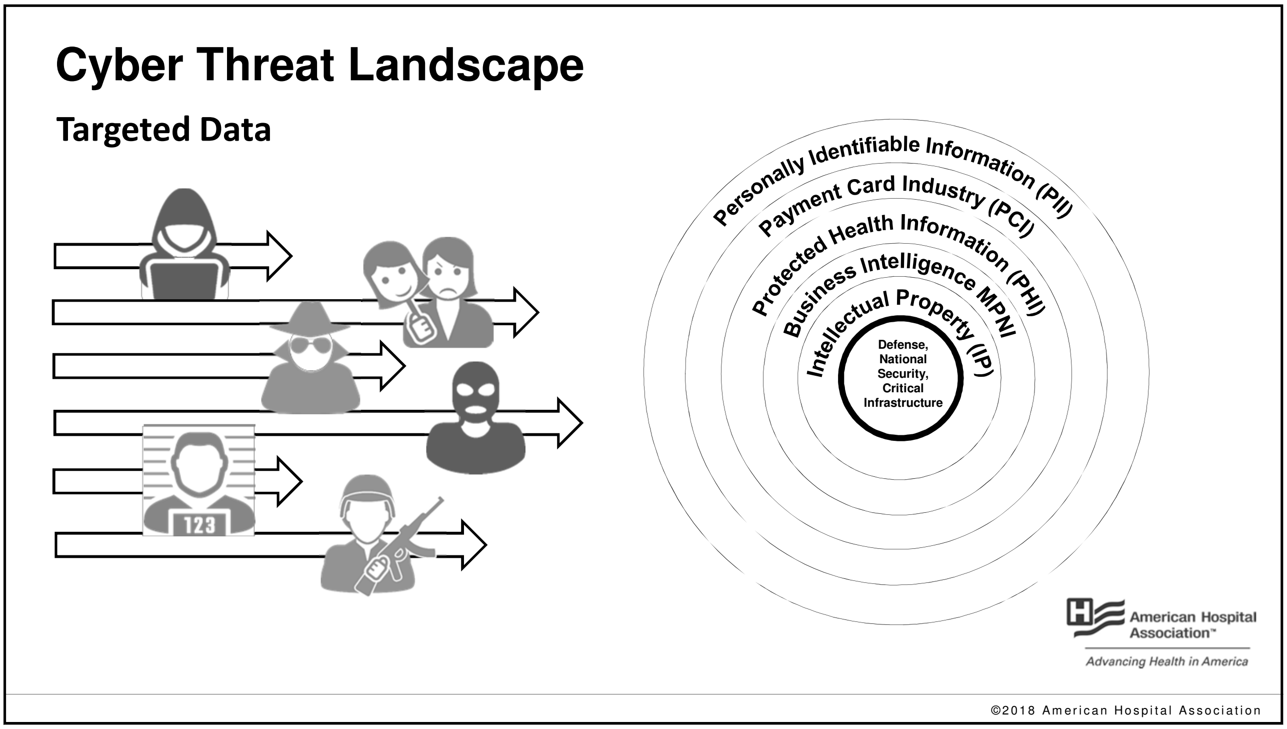
INSIDER
Insider threat actors typically steal proprietary information for personal, financial or ideological reasons.

CRIME
Individual and sophisticated criminal enterprises steal personal information and extort victims for financial gain.

ESPIONAGE
Nation-state actors conduct computer intrusions to steal sensitive state secrets and proprietary information of economic or national security interest.

WARFARE
Nation-state actors conduct computer intrusions to collect intelligence on and/or sabotage critical infrastructure in advance of future offensive action.

American Hospital Association™
Advancing Health in America



Cyber Threat Landscape

Targeted Data

Personally Identifiable Information (PII)

Payment Card Industry (PCI)

Protected Health Information (PHI)

Business Intelligence MPNI

Intellectual Property (IP)

Defense, National Security, Critical Infrastructure

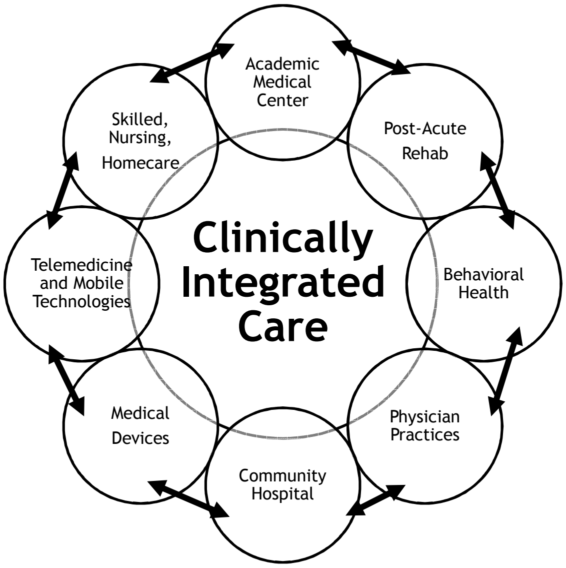
American Hospital Association™
Advancing Health in America

Recent FBI and DHS Alerts on Nation State Cyber Threats

- 8/9/2018 – FBI and DHS update on HIDDEN COBRA – North Korean Government Trojan malware variant KEYMARBLE
- 7/30/2018 - DHS webinar on Russian government cyber activity targeting US critical infrastructure including the energy grid,
- 6/14/2018 - Trojan malware variants – referred to as TYPEFRAME The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA.
- 6/4/2018 – Malware found in thumb drives manufactured in China. Supply chain issues.
- 5/29/2018 – HIDDEN COBRA destructive malware and RAT attributed to North Korea
- 5/23/20918 – VPNfilter malware targeting routers and energy grid attributed to Russia.
- 4/17/2018 - Orangeworm Group, Kwampirs malware (suspected nation state activity) Malware *found on medical imaging devices*. Supply chain attack.
- 3/23/2018 - Indictment of Iran, IRGC affiliated actors – Mabna Institute
- 12/19/2017 - Wannacry ransomware, propagated through unpatched medical devices, attributed to North Korea
- 7/1/2017 – Petya/NotPetya – ransomware attributed to the Russian Military – GRU. (Nuance Communications)

American Hospital Association™
Advancing Health in America

Emerging And Embedded Cybersecurity Risk



- Various forces – including the move toward payment tied to quality, clinical outcomes and episodes of care – are driving clinical integration across provider types, leading to new and more complex data sharing and integration requirements for providers. Clinical integration also includes telemedicine and mobile technologies.

American Hospital Association™
Advancing Health in America

Risk Considerations

Top 12 Risk Considerations for Leadership

Patient Safety & Mission Critical Systems

- **Mission-critical systems, devices and networks related to patient safety and care delivery - first and always!**
- Cyberattack vulnerability?

#1

Strategic Cyber-Risk Profile

- Strategic cyber-risk profile, from the adversaries' perspective.
- Main cyber adversaries based upon patients, data sets and network connections.
- ***Who is coming after us?***

#2

Tactical Cyber- Risk Profile

- Current state tactical cyber-risk profile based on our latest risk assessments and vulnerability and penetration testing?
- ***Polices, procedures risk assessment vs. technical risk assessment***

#3

Prioritization

- Prioritization of cybersecurity policies, procedures, controls and technical risks - patient safety and care delivery first, data protection second, business operations third?

#4

Capabilities

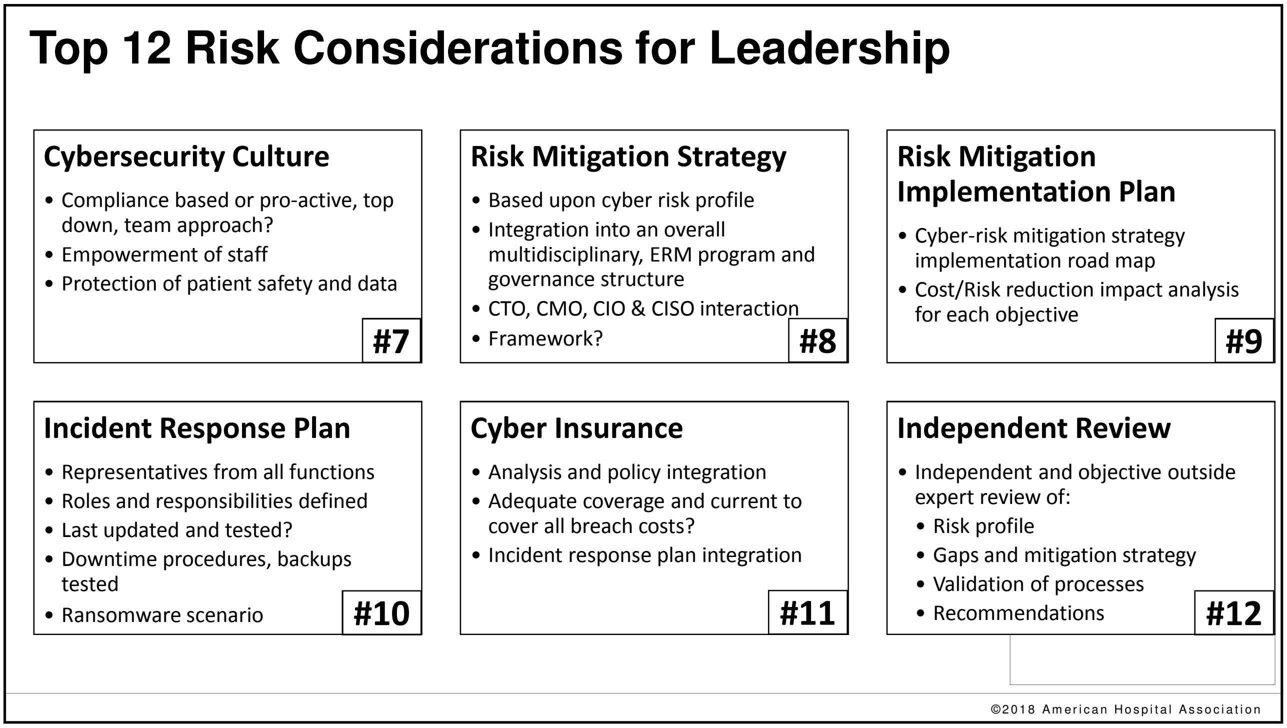
- Sufficient and capable human and technical resources?
- Sufficient budget devoted to our information-security program?
- ***CISO reporting structure***

#5

Vendor Risk-Management Program

- Recent in-depth technical, legal, policy and procedural, review
- Vendor cyber risk exposure – access to networks, data and ***mission criticality***

#6



Top 12 Risk Considerations for Leadership

Cybersecurity Culture

- Compliance based or pro-active, top down, team approach?
- Empowerment of staff
- Protection of patient safety and data

#7

Risk Mitigation Strategy

- Based upon cyber risk profile
- Integration into an overall multidisciplinary, ERM program and governance structure
- CTO, CMO, CIO & CISO interaction
- Framework?

#8

Risk Mitigation Implementation Plan

- Cyber-risk mitigation strategy implementation road map
- Cost/Risk reduction impact analysis for each objective

#9

Incident Response Plan

- Representatives from all functions
- Roles and responsibilities defined
- Last updated and tested?
- Downtime procedures, backups tested
- Ransomware scenario

#10

Cyber Insurance

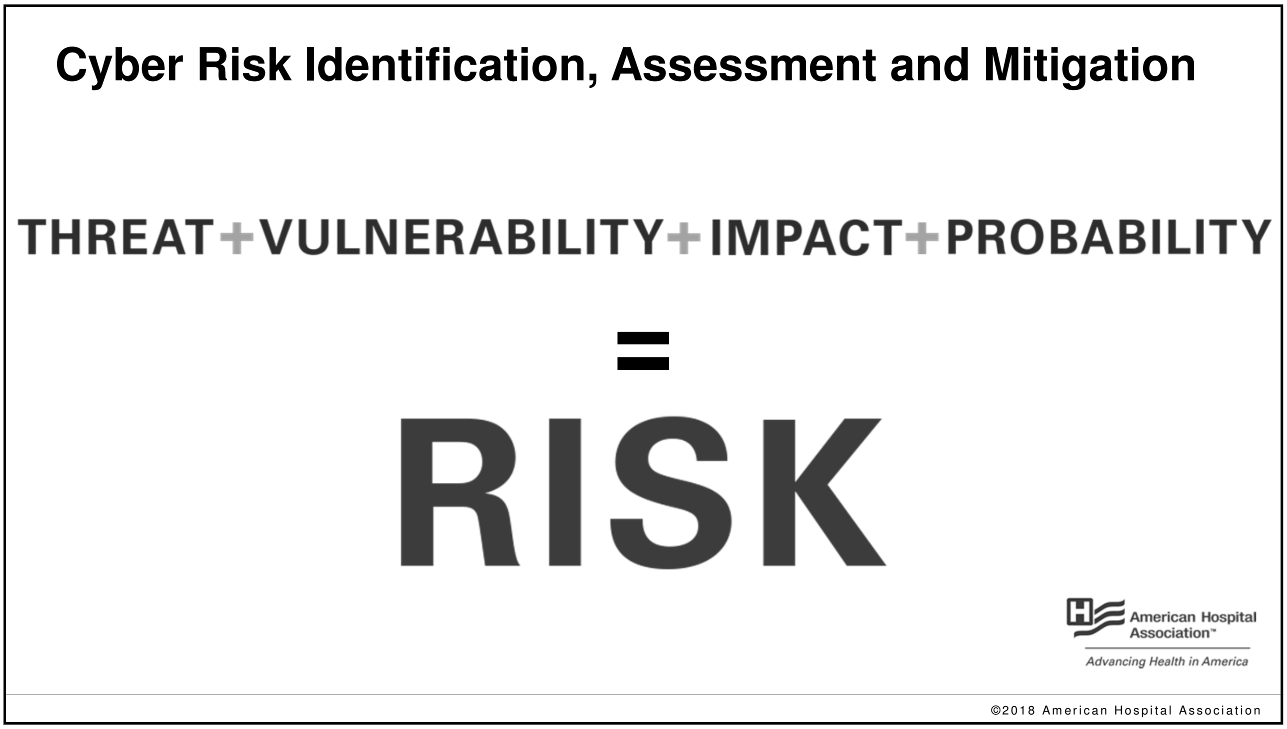
- Analysis and policy integration
- Adequate coverage and current to cover all breach costs?
- Incident response plan integration

#11

Independent Review

- Independent and objective outside expert review of:
  - Risk profile
  - Gaps and mitigation strategy
  - Validation of processes
  - Recommendations

#12



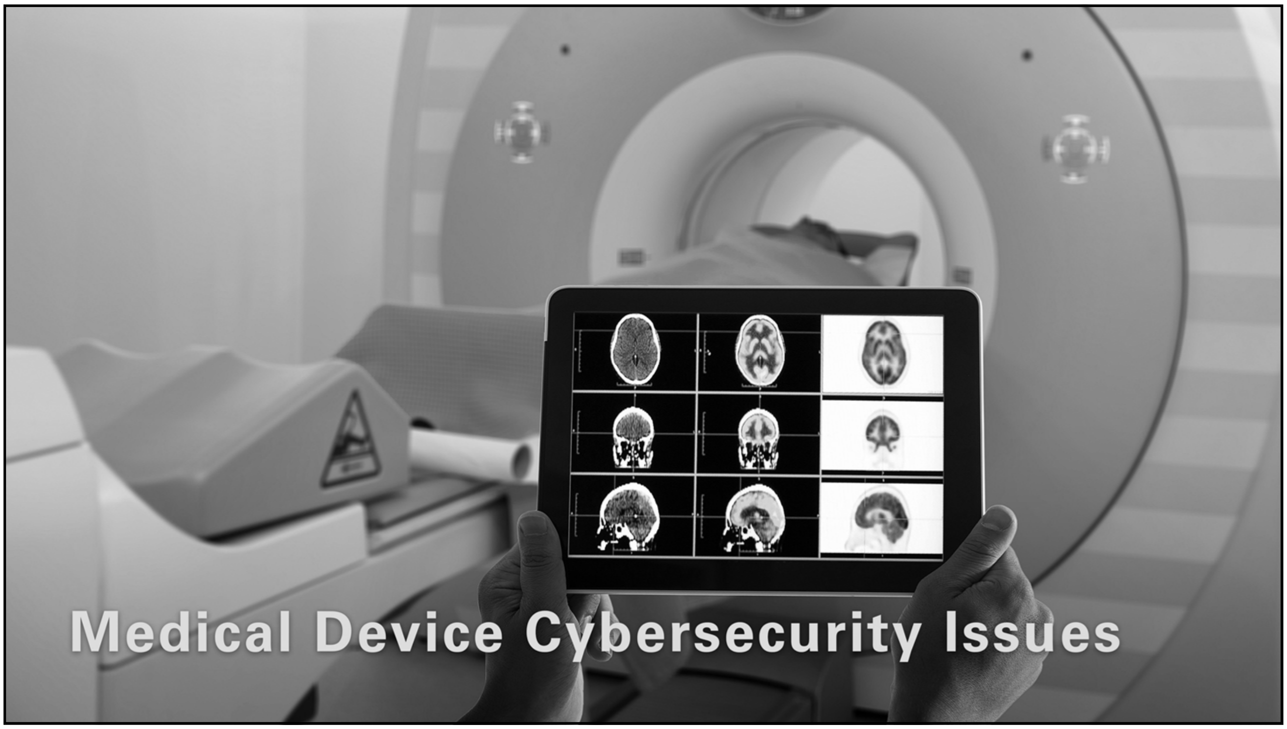
Cyber Risk Identification, Assessment and Mitigation

THREAT + VULNERABILITY + IMPACT + PROBABILITY

=

RISK

American Hospital Association™
Advancing Health in America

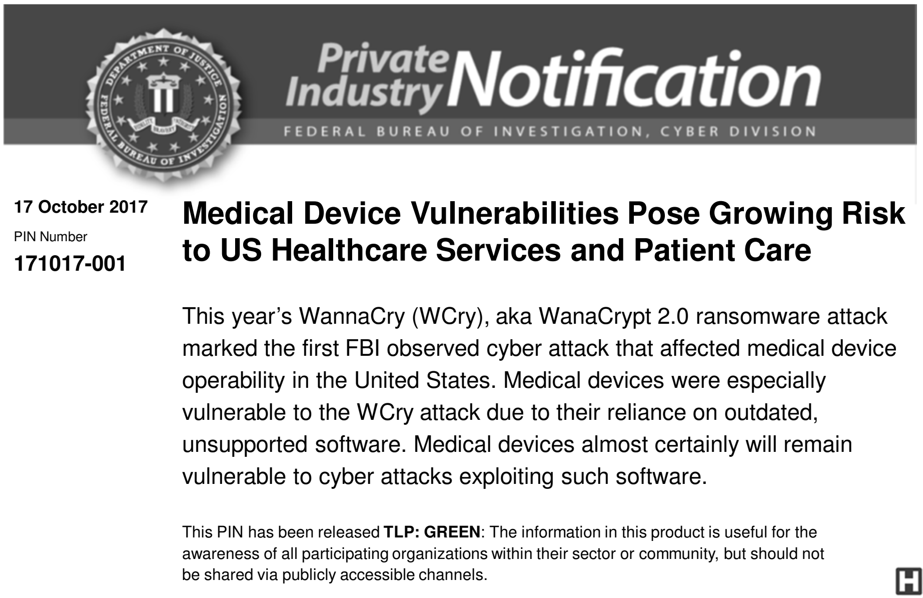


Medical Device Cybersecurity Issues

Threats And Challenges

- **Patient Safety and Delivery of Care**
- Connected devices
- Ransomware
- Attack vector for other malware
- Theft of PHI on devices
- Network access
- Intentional or unintentional impact of malware on accurate function of device
- Data integrity
- Unsegregated device network
- Inventory
  - Shadow IT – hidden networks
  - BYOD policy
- Legacy devices – end of life use
  - Lack of software bill or particulars and supported lifetimes
- Outdated operating systems
- Patch management
- Device access
- Lack of clear responsibility
  - Manufacturer – Vendor – Provider
  - FDA Pre and Post Market Guidance
- Lack of security by design
- Information Technology vs Medical Technology
  - Mission critical systems
  - CIO or CISO vs CTO or CMO?
- AHA efforts

American Hospital Association™
Advancing Health in America



Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

17 October 2017

PIN Number

171017-001

Medical Device Vulnerabilities Pose Growing Risk to US Healthcare Services and Patient Care

This year's WannaCry (WCry), aka WanaCrypt 2.0 ransomware attack marked the first FBI observed cyber attack that affected medical device operability in the United States. Medical devices were especially vulnerable to the WCry attack due to their reliance on outdated, unsupported software. Medical devices almost certainly will remain vulnerable to cyber attacks exploiting such software.

This PIN has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

American Hospital Association™

Advancing Health in America

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

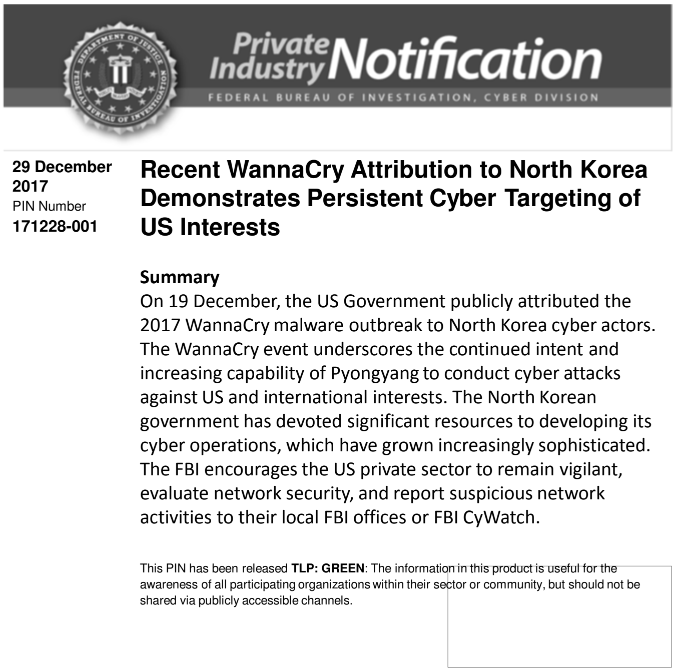
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

SONY



Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

29 December 2017

PIN Number

171228-001

Recent WannaCry Attribution to North Korea Demonstrates Persistent Cyber Targeting of US Interests

Summary

On 19 December, the US Government publicly attributed the 2017 WannaCry malware outbreak to North Korea cyber actors. The WannaCry event underscores the continued intent and increasing capability of Pyongyang to conduct cyber attacks against US and international interests. The North Korean government has devoted significant resources to developing its cyber operations, which have grown increasingly sophisticated. The FBI encourages the US private sector to remain vigilant, evaluate network security, and report suspicious network activities to their local FBI offices or FBI CyWatch.

This PIN has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Cyber Insurance

Cyber Insurance Considerations

- Do we need it? Yes!
- How much is enough?
- Risk Profile
  - Risk transfer
- Existing Coverage Analysis
  - Interaction of policies
    - Crime, Fraud
- Evaluation of Underwriters
- Coverage
- Digital asset valuation
- Continuity of operations
- Response, remediation and recovery
- Forensics firm – qualified panel?
  - Included in Incident Response Plan?
- Responsiveness
- Other coverages
  - Victim notification and credit monitoring.
  - Social engineering coverage
  - Ransomware - payment permission?
  - Cyber extortion
  - Management liability
  - Management personal coverage
  - Third party vendor liability

American Hospital Association™
Advancing Health in America

Take Aways

Take Aways

- Cybersecurity is not just an IT issue focused on risk to the security and privacy of patient data – It is an enterprise risk management issue.
- The cybersecurity culture of the organization – the people, are best defense or weakest link, and the most cost effective defensive measure.
- Money can’t cure reputational harm.
- Cybersecurity risk is constantly evolving, outpacing defensive measures and can never be eliminated, only mitigated.
- Therefore, threat detection, time to detection from intrusion, incident response and recovery plans are critical.

American Hospital Association™
Advancing Health in America

Take Aways

- Understand the organization may have embedded cyber risk beyond their control – (e.g. Allscripts, Nuance Communications, the energy grid.)
- Know your risk profile, have a constantly evolving cybersecurity strategy and execution roadmap.
- All cybersecurity issues should be first viewed as and prioritized within the context of **impact to patient safety and delivery of care first**.

American Hospital Association™
Advancing Health in America

We Are Here For You

American Hospital Association™
Advancing Health in America

Cybersecurity and Risk Services

To help protect your privacy, PowerPoint has blocked automatic download of this picture.

To help protect your privacy, PowerPoint has blocked automatic download of this picture.

To help protect your privacy, PowerPoint has blocked automatic download of this picture.

To help protect your privacy, PowerPoint has blocked automatic download of this picture.

Questions And Discussions

jriggi@aha.org

(O) +1 202-626-2272

(M) +1 202-640-9159 (**24 hours**)

800 10th Street N.W. Suite 400
Washington, D.C. 20001