Presenting the Case for Cybersecurity Education of Clinicians

Session 149; February 13, 2019

UT Southwestern Medical Center®

Axel Wirth, CPHIMS, CISSP, HCISPP
Distinguished Technical Architect, Symantec Corporation

Symantec™

Joseph H. Schneider, MD, MBA
Assistant Professor, University of Texas Southwestern, Dallas

Conflict of Interest

Joseph H Schneider, MD, MBA has no real or apparent conflicts of interest to report.

Axel Wirth, CPHIMS, CISSP, HCISPP is employed by Symantec, a cybersecurity vendor, but has no real or apparent conflicts of interest to report.

Learning Objectives & Agenda

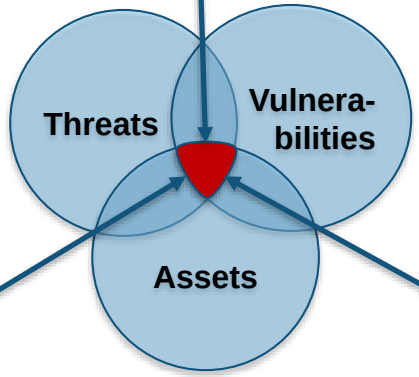
- Discuss the complexities of today's cybersecurity challenges and how they impact healthcare organizations on many levels
- Define the cybersecurity responsibilities, and consequently educational needs, of non-technical stakeholders
- Analyze clinicians' role in today's cybersecurity environment, ranging from patient care decisions to incident response
- Axel will present first, followed by Dr. Joe

Session sponsored by HIMSS Collaborator: American College of Clinical Engineering (ACCE)

Healthcare Cybersecurity

A Growing Risk – But Why and Why Now?

Growing Cyber-Risks



Today's Threats:

- Actors: *Cyber-Criminals, Cyber-Activists, Nation States, Hackers for Hire*
- Motivation: *Financial, Political, Economic*
- Attacks: *Targeted, Sophisticated, Stealthy, Well-Executed*

Vulnerabilities:

- Growing Attack Surface
- Increasing Complexity: *ACO's, EHR Adoption, Home Care, Medical Device Networks,*
- Integration creates: *Dependency, Single Points of Failure*
- Technology adoption: *Cloud, Mobile, IoT, AI, Blockchain, ….*

Changing Motivation

Higher Impact Potential

Assets:

- Traditional: *Information, Money, Identities*
- Evolving: *Infrastructure, Society, Economy*
- Indirect: *Care Delivery, Patient Safety, National Security*

Cybersecurity in 2019

Know Thy Enemy – What They are After

- Cybercrime as a Business / Cybercrime impacting Business
  - Underground Economy: ~$1.5 Tn annual profit (Dr. M. McGuire: U of Surrey)
  - Global economic losses estimated to be ~$1-3 Tn (range of a few % of GDP)
- Cyber Warfare and Activism
  - Attacks as a political statement - Anonymous hacktivists group attacked Boston Children's Hospital (2014) & Hurley Medical Center (2016, Flint, MI)
- Intellectual Property
  - Clinical trials, research, designs, formularies, software code, …
- Attacks may or may not be targeted
  - Victim simply may fit exploit profile
  - Or, may be looking for easy prey and healthcare may fit the bill
- Insider Threats
  - ID Theft, Negligence, …. Patients

Cybersecurity in 2019

Know Thy Enemy – Many Opportunities

Attack Complexity and Impact

WIRED

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

.....

The result was more than $10 billion in total damages, according to a White House assessment confirmed to WIRED by former Homeland Security adviser Tom Bossert, who at the time of the attack was President Trump's most senior cybersecurity-focused official. Bossert and US intelligence agencies also confirmed in February that Russia's military—the prime suspect in any cyberwar attack targeting Ukraine—was responsible for launching the malicious code. (The Russian foreign ministry declined to answer repeated requests for comment.)

To get a sense of the scale of NotPetya's damage, consider the nightmarish but more typical ransomware attack that paralyzed the city government of Atlanta this past March: It cost up to $10 million, a tenth of a percent of NotPetya's price. Even WannaCry, the more notorious worm that spread a month before NotPetya in May 2017, is estimated to have cost between $4 billion and $8 billion. Nothing since has come close. "While there was no loss of life, it was the equivalent of using a nuclear bomb to achieve a small tactical victory," Bossert says. "That's a degree of recklessness we can't tolerate on the world stage."

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Many Opportunities to Monetize

Cyber extortionists 'The Dark Overlord' offering celeb plastic surgery photos

The criminals' sophisticated PR strategy is designed to increase the pressure on victims to pay extortion demands.

10:43 UK
Friday 04 January 2019

The criminals are offering photos of cosmetic surgery. File pic.

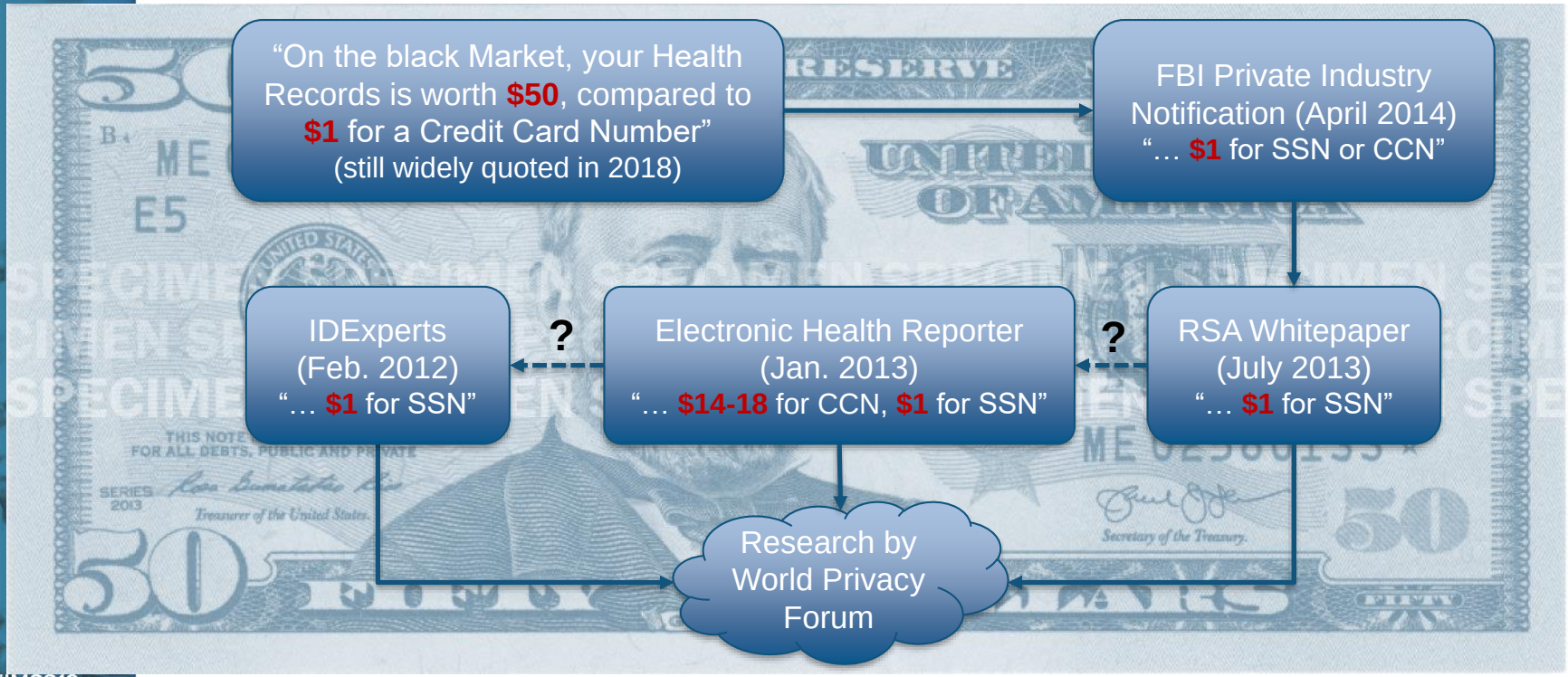
By Alexander J Martin, technology reporter

A cyber crime group calling itself "The Dark Overlord" is offering stolen celebrities' cosmetic surgery photographs to the media to bolster an extortion campaign targeting the celebs themselves.

https://news.sky.com/story/cyber-extortionists-the-dark-overlord-offering-celeb-plastic-surgery-photos-11597618/

Cybersecurity in 2019

Value of Health Data in the Underground Economy – Myths



Cybersecurity in 2019

Today's Reality is Far More Complex

fedscoop

Hacker puts more than 9M health care records up for sale on the dark web

From a few $'s to $1,000 …
to free …

… to unquantifiable.

Forbes

Your Electronic Medical Records Could Be Worth $1000 To Hackers

DataBreaches.net

May 04 2017

TheDarkOverlord dumps 180,000 patients' records from 3 hacks

Posted by Dissent at 7:46 pm Breach Incidents, Commentaries and Analyses, Hack, Health Data, Of Note, U.S.

While thousands of their followers on Twitter seem to be eagerly waiting for TheDarkOverlord (TDO) to dump more tv films or episodes of popular series, TDO went non-fiction this morning, dumping patient/medical records from some of their hacks in the healthcare sector last year. All told, almost 180,000 patients had their personal information shared with the world.

Healthcare Cybersecurity – What is Different?

A Cybersecurity Expert's View

Healthcare is viewed as less Security Mature than other Industries

- (although that is a pretty low bar to clear - Target, Equifax, Marriott, etc.)
- Healthcare: ¾ of hospitals spend <6% of their IT budget on security
- Security mature industries spend 10% - 12% of IT budget

BUT - Enforcing Security is more difficult than Elsewhere

- Complexity is your enemy – and healthcare is quite complex:
  - Organizational – impact on decision making and enforcement
  - Technical – number of vendors, devices, platforms, etc.
- Employment status, workflows, and equipment needs:
  - Contracted vs. employed
  - Changing roles & privileges, shared accounts, mobility, etc.
- Difficulty of enforcing security and compliance:
  - Strict enforcement can impact care delivery
  - Maintenance challenges (patching) and legacy devices

What HIPAA Taught Us

Confidentiality, Integrity, Availability – Really?

- HIPAA trained us well: **C** – I – A (e.g., Breach Notification Rule)
- Shifting Global Threats are leading to changing Security Priorities:
  - From accidental incidents to targeted and malicious attacks
  - Changing motivation: criminal attacks, political objectives
  - Complex objectives and targets: devices, information, trust

	Confidentiality	Availability	Integrity
Past	Negligence, or lost or stolen devices	Technical failure	Accidental alteration of data
Now	• Skilled adversaries with a mission • Criminal intent (ransom, blackmail) • Political attacks (nations, hacktivists)	Care delivery, e.g.: • Ransomware • Medical Devices	• Targeted attacks: intent to harm • Create doubt in data (and larger healthcare system)

Lesson learned: Compliance does not guarantee sufficient Security

"Compliance only works if your enemy is the compliance auditor"

Ted Harrington, Independent Security Evaluators

Security Scenarios – Example 1
"I see the Cloud from Both Sides Now"

Understanding Cloud Adoption – and Security Implications

- Controlled (e.g., EHR migration) – compliance and security *should* be part of the design process and architecture
- Uncontrolled (e.g., file sharing) – this is the more difficult one to address; plenty of security, privacy, and compliance risks

Need to Assure Confidentiality, Integrity, Availability in Both Scenarios

- Technologies at play (adopted for the cloud use case):
  - Network security (data in motion)
  - Endpoint security (data at rest, e.g. cloud workloads)
  - Encryption (at rest and in motion)
  - Data Loss Prevention (at rest and in motion)
  - CASB (Cloud Access and Security Broker) – works with or includes several of the above
- How do you protect data that doesn't even traverse your enterprise?
  - Controlling and securing cloud-to-cloud traffic
  - 5G is around the corner and will make this even worse

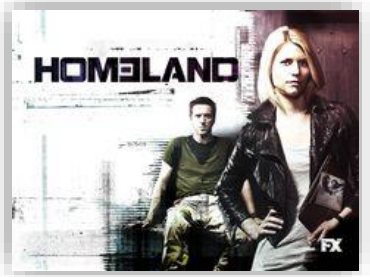
Security Scenarios – Example 2
Medical Device Cybersecurity

What are the Risks?

- Patient Safety – plenty of security research but no reported case of patient harm
  - But feasible and plausible – no need to panic, but proceed with a sense of urgency
- Care Delivery – many reported, e.g. CathLab shutdown; WannaCry (UK NHS)
- Device as the weakest link – reported beachhead attacks
- Other risks: privacy, reputation, financial
- Likely scenario – incident resulting from a non-targeted event

Industry and Regulatory Action

- FDA Pre and Post Market Cybersecurity Guidance
- Developing efforts in China, Canada, EU
- Healthcare Providers are launching Cybersecurity Initiatives
- Device Manufacturers developing Security Strategy and Expertise
- Stakeholder cooperation – e.g. vulnerability sharing



Note: HIPAA C-I-A limited to **PHI**

- Insufficient for medical devices:
  - Consider non-PHI risks:
    - data not attributed to specific or identifiable patients
    - technical device data (calibration, safety limits …)

Healthcare Cybersecurity - Recap

Why are Health Organizations and Data a Target?

- Rich information
- Longtime value
- Perceived low defenses
- Many entry points
- Many ways to monetize
- Valuable Intellectual Property:
  - Competitive advantage
  - Economic differentiator
- Pressure to restore operations (Ransomware)

Attractors

- Difficult and slow to monetize
- Utilization requires skill and patience
- Saturated underground market
- (Moral concerns)

Detractors

Healthcare Cybersecurity - Recap

Clinician Cybersecurity Leadership

Administrative Role	• Security Strategy and Governance • Procurement Decisions • Replacement Planning
Enablement Role	• Education • Peer Leadership
Public Role	• Public Face / Communication • Patient Advisory and Advocacy
Security Role	• Security Incident Response • Security Research

As adversaries change, our cyber defenses needs to adopt, too.
Remember – Minutemen used to work well … but not anymore.

Cybersecurity Is Like Herding Cats…

A Clinician and Informaticist's View

Limited incentives for vendors/device makers to make incidents public

No central repository for vulnerabilities and incident reporting

Healthcare CIOs can't keep up with patching

Clinicians generally don't appreciate risks

Limited awareness of security impact on safety and efficiency

Executives, lawyers & compliance poorly understand cyber-risks

A Quick View of How Clinicians Deal with Cybersecurity – At Least Enough to Cause Problems…

We Use The Weakest Passwords
…That We Can

- 123456
- password
- 123456789
- 12345678
- 12345
- 111111
- 1234567
- sunshine
- qwerty
- iloveyou

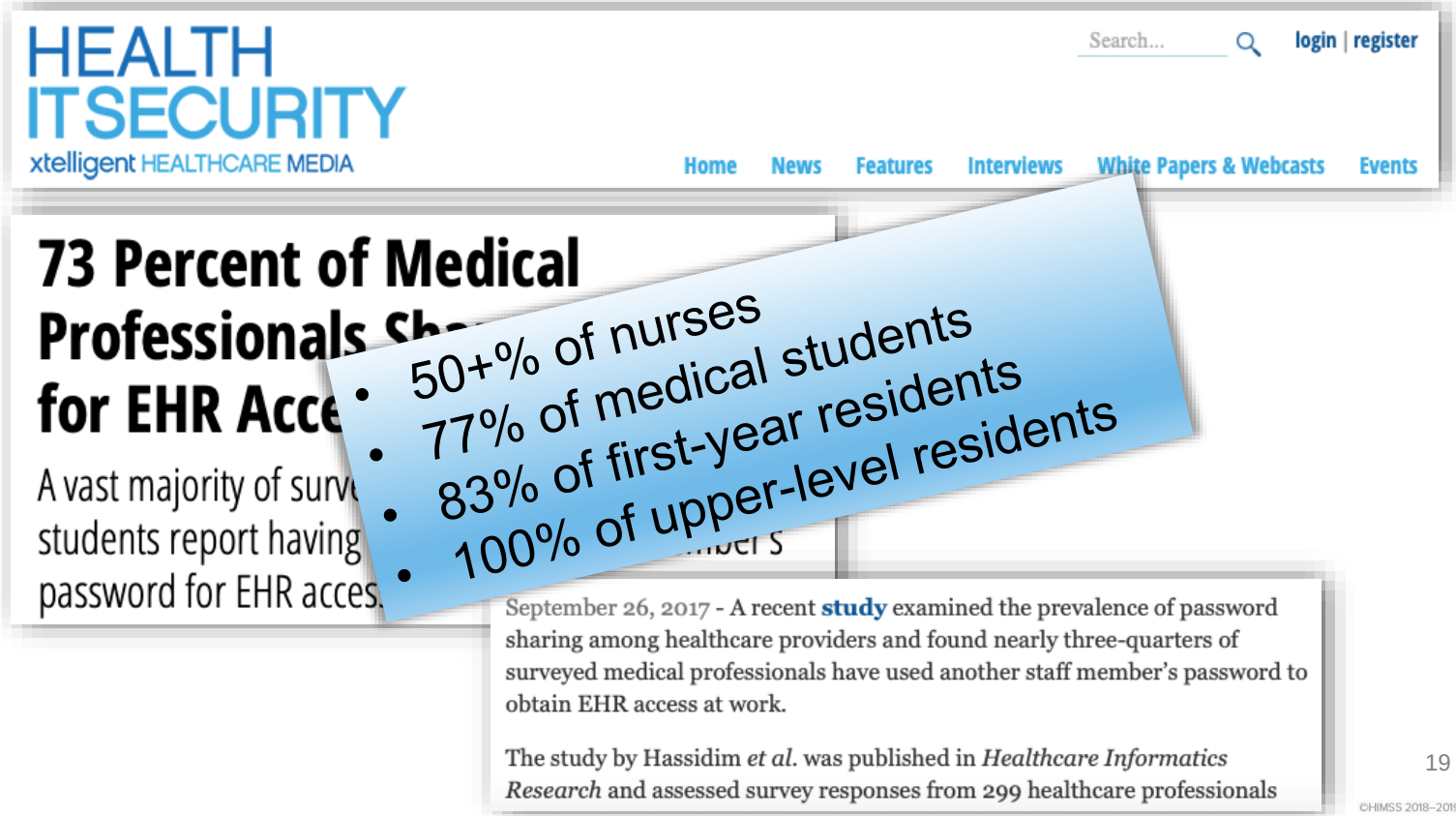
#HIMSS19

We Write Passwords Down

… As They Become Harder to Memorize

We Share Our Passwords

… Especially When "Locked Out"

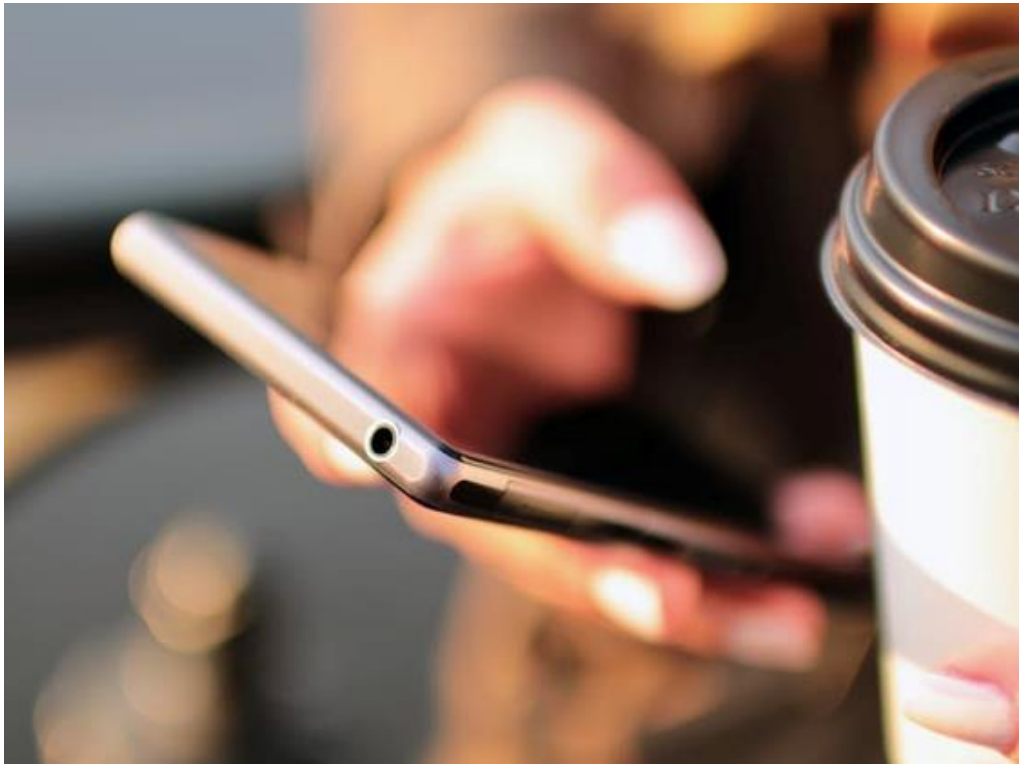


We Click Through Online Training

… As Quickly as We Can to Get Through it

We Text & e-mail PHI Regularly

… Because Secure Systems are Hard to Use



Enough Clinicians Feel That…
(At Least Enough to Be a Big Problem)

- Cybersecurity is “not my job”
- Annual security training classes or programs are a waste of time
- IT/Biomed is more concerned with eliminating all risk rather than balancing it with patient safety
- IT/Biomed doesn’t understand the challenges they create
- We doubt that we can be protected

Technology

Providers lack confidence in medical device cybersecurity

By Rachel Z. Arndt

MORE THAN HALF of provider organizations lack a strong degree of confidence in their medical device security, according to a survey by KLAS Research and the College of Healthcare Information Management Executives.

That's what happened with the WannaCry ransomware in May 2017, when hackers targeted computers running outdated versions of Microsoft Windows.

"Medical device manufacturers make every effort to address cybersecurity throughout the product lifecycle," said a spokesperson from the Advanced Med-

Clinicians Undervalue Cyberrisk Prevention

Some Hypotheses Why This is so:

- We highly value patient safety
- We highly value efficiency (e.g., 40% of healthcare workers would allow a colleague to use their work computer)
- Our education and organizations generally don't support connecting cyberrisk with patient safety/efficiency
- Like adolescents, we undervalue risks that aren't apparent
- Our informatics leaders (CMIOs) are not focused on cybersecurity

What CMIOs Focus On
2008 and 2014

Source: AMDIS-Gartner CMIO Role Survey

What CMIOs Focused On In 2017

Cybersecurity is Still Not on the Radar

Source: AMDIS-Gartner CMIO Role Survey

Some Physicians Want To Help
There is Hope

- Abbott/Chertoff 2018 study of 300 physicians:
  - 92% - keeping data secure is a focus of their hospital
  - 71% - cybersecurity is a shared responsibility
  - **75% - feel ill-prepared** to mitigate cyber risks
  - Only 15% report having seen or read advisories related to medical device security in the last six months

- Report recommendations:
  - *Create standards and cybersecurity by design*
  - *Invest in cybersecurity incident response processes*
  - ***"Improve education, focus & training to increase all stake-holders' understanding of cyber risk..."***

HHS: Cybersecurity Is Public Health Issue

Task Force Recommended Goals

1. Define and streamline cybersecurity leadership, governance, and expectations
2. Identify strategies to protect R&D efforts and intellectual property from attacks or exposure
3. Improve information sharing of industry threats, weaknesses, and mitigations
4. Improve staffing necessary to prioritize and ensure cybersecurity awareness and technical capabilities
5. *Increase cybersecurity awareness and education*
6. Increase security & resilience of medical devices and health IT

Cybersecurity Task Force Report

What Would A Better Culture Look Like?

Organizational & Clinical Leaders Could…

- Position cybersecurity as part of patient safety & effectiveness
- Focus on identifying and reducing cybersecurity “hassles”
- Make education a “painless” daily thing, not an “annual competence” and reward risk identification
- Provide support for CMIOs and other clinicians to help IT/Biomed
- Support trained clinicians as equal partners in the cybersecurity decision-making process
- Consider cybersecurity misbehavior as the equivalent of providing bad clinical care, not an administrative infraction

Add Clinicians To Cybersecurity Leadership

Axel Wirth's Proposed Framework

Administrative Role	• Security Strategy and Governance • Procurement Decisions • Replacement Planning
Enablement Role	• Education • Peer Leadership
Public Role	• Public Face / Communication • Patient Advisory and Advocacy
Security Role	• Security Incident Response • Security Research

Add Clinicians To Cybersecurity Leadership

The Story of Dr. RK

Administrative Role

- Security Strategy and Governance
- Procurement Decisions
- Replacement Planning

- Dr. RK, an interventional cardiologist, became frustrated with the seemingly arbitrary “rules” imposed on clinicians by IT Security
- CMIO worked with CIO for Dr. RK to co-chair the “Clinical Data Access Team (CDAT)” that handled privacy & security decisions
- Dr. RK took shared responsibility for issues that impacted clinical care, delivered tough cybersecurity messages to physicians and stood side-by-side with IT Security and Biomed
- Compensated at ~ 40% of earnings, but it was adequate
- Dramatically improved perceived quality of security decisions and the relationship of IT Security with other clinicians

Add Clinicians To Cybersecurity Leadership

The Story of Dr. DM

Enablement Role	• Education • Peer Leadership

- Dr. DM, an OB/GYN, became frustrated with the “unfriendliness” of HIT training and messaging for physicians
- CMIO worked with the Education VP to get Dr. DM onto HIT Education Team
- With Dr. DM’s support, the team built simple and effective education tools, especially videos of physicians speaking to physicians
- Compensated at ~ 40% of earnings, but it was adequate
- Dramatically improved the quality of HIT education and the relationship of the Education Team with clinicians

Add Clinicians To Cybersecurity Leadership

Other Things Clinicians Like Dr. DM can do:

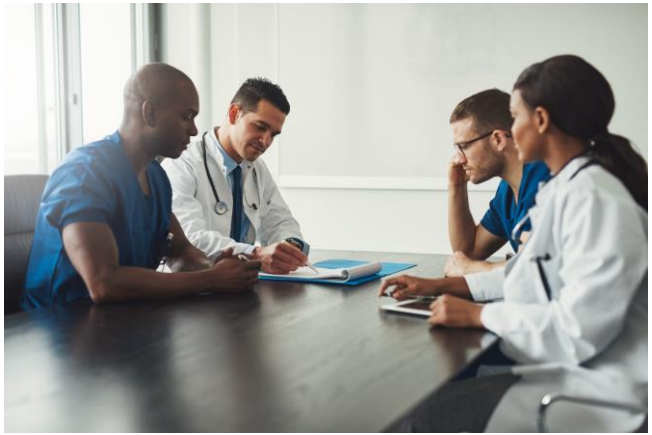
Enablement Role	• Education • Peer Leadership

- Find the patient safety impacts of all proposed cybersecurity changes/announcements
- Construct the best messaging and methods to “catch” the clinician’s focus (it’s not e-mail)
- Build cybersecurity education into the clinician’s regular activities
- Construct meaningful reward programs for reporting cybersecurity weaknesses
- Build rapport by referring to physicians, nurse practitioners & physician assistants by their titles (or as “clinicians”) rather than as “providers” or ”mid-levels”

Doctors and Clinicians Learn As Adults

They Learn Best when Learning:

- Is self-directed & they are ready
- Is from experience
- Addresses “real” situations
- Can be applied quickly



Add Clinicians To Cybersecurity Leadership

Clinicians are Your Best Representatives

Public Role	• Public Face / Communication • Patient Advisory and Advocacy

- Cybersecurity is increasingly impacting patients (e.g., pacemaker recall over security issue)
- Physicians typically are having discussions with patients about their care and should begin to bring cybersecurity into these
- Physician/clinician informatics groups (e.g., AMIA, AMDIS, professional organizations) can prepare national positions where appropriate
- The Dr. RKs and DMs can help with local messaging
- Having patients represented in cybersecurity decision-making is a next step

Add Clinicians To Cybersecurity Leadership

Other Things Clinicians Like Dr. RK can do:

Security Role	• Security Incident Response • Security Research

- Lead root cause analyses regarding cybersecurity/patient safety issues, preferably handled in the Patient Safety Organization
- Work with IT/Biomed in managing incidents to help them understand the impact of proposed actions
- Serve as the co-spokesperson during cybersecurity incidents
- Identify weaknesses
- Construct protected time for IT/Biomed staff to join clinical rounds with physicians, nurses, NPs, etc. to understand their workflow and the importance of rapid and easy data access

CMIOs Need To Focus On Cybersecurity Too

Things CMIOs can do:

- Connect with CIOs/CISOs and let them know we value cyber-security
- Lobby for funding for cyber-clinicians – the Dr. RKs/DMs
- Encourage AMDIS, AMIA, ANIA and other clinical informatics organizations to engage with national programs, with educational materials (e.g., how to work with your CISO) and speakers
- Engage professional clinical/medical societies both nationally (e.g., the ANA, AAP) and locally (e.g., the Texas Medical Association)
- Have your CEO/COO/CMO/CNO provide medical staff/nursing recognition to clinical cyber-security leaders

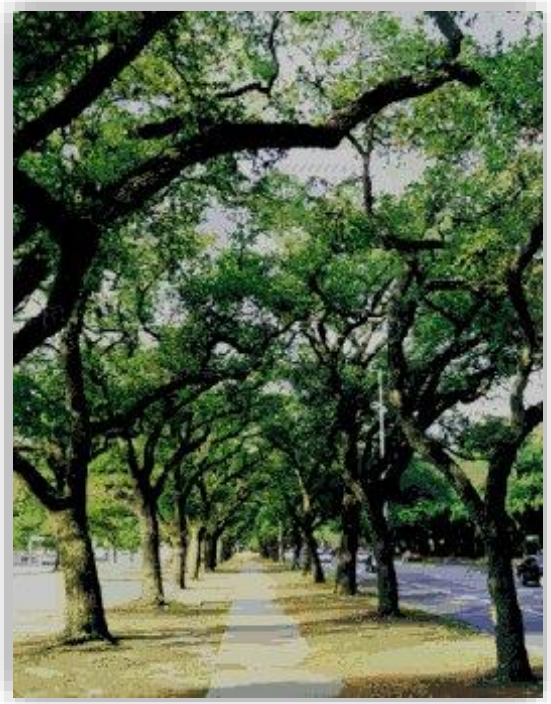
Identifying Clinical Cybersecurity Leaders
But – Takes Work to Develop Them

- These physicians/clinicians are not unique
- Often “too busy”/too scared (?) to step forward if not encouraged
- Issues to consider:
  - How do you find them?
  - What do you want them to do (domain versus local experts)
  - How do you compensate them?
  - How do you build their competence?
  - How do you measure their success?
  - How do you build their reputation in the organization?
  - What is their career path?

Thank You For Your Time
Questions?

Dr. Joe Schneider, *drjoes1tx@gmail.com*

Axel Wirth, *axel_wirth@symantec.com*



Please complete the online session evaluation

#HIMSS19