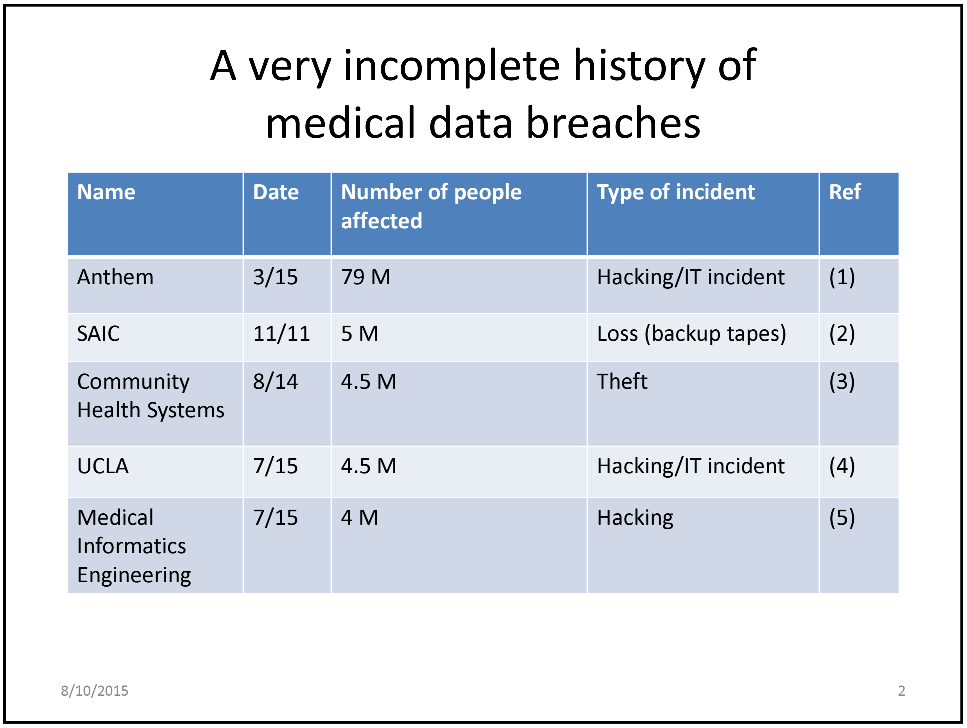
An Expanding Threat Spectrum for Health Information Technologies: Starting a Conversation

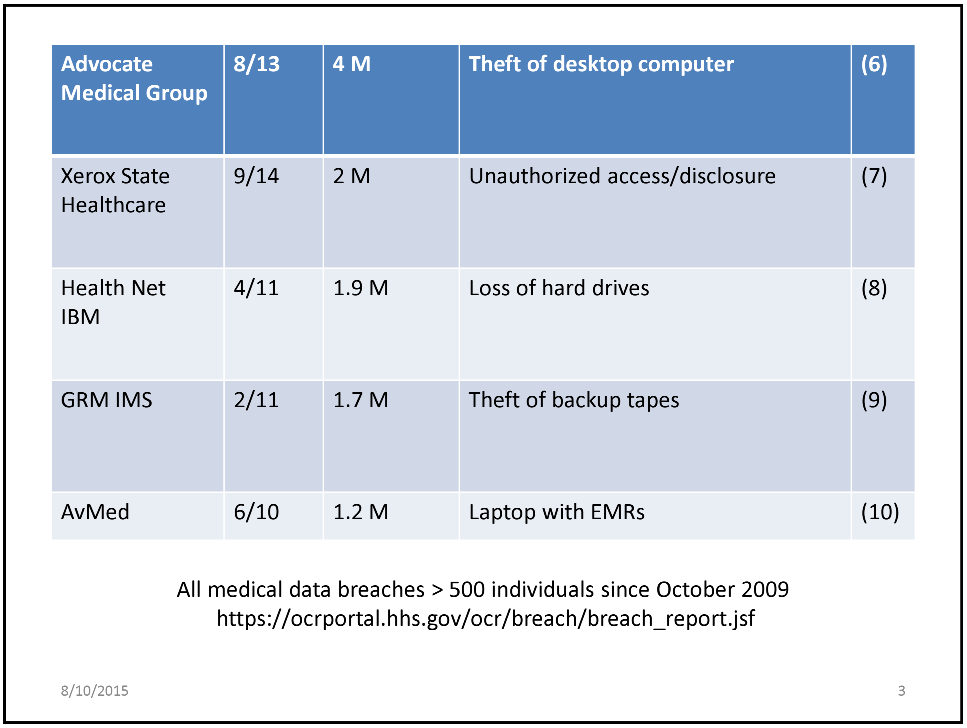
Herb Lin

Stanford University



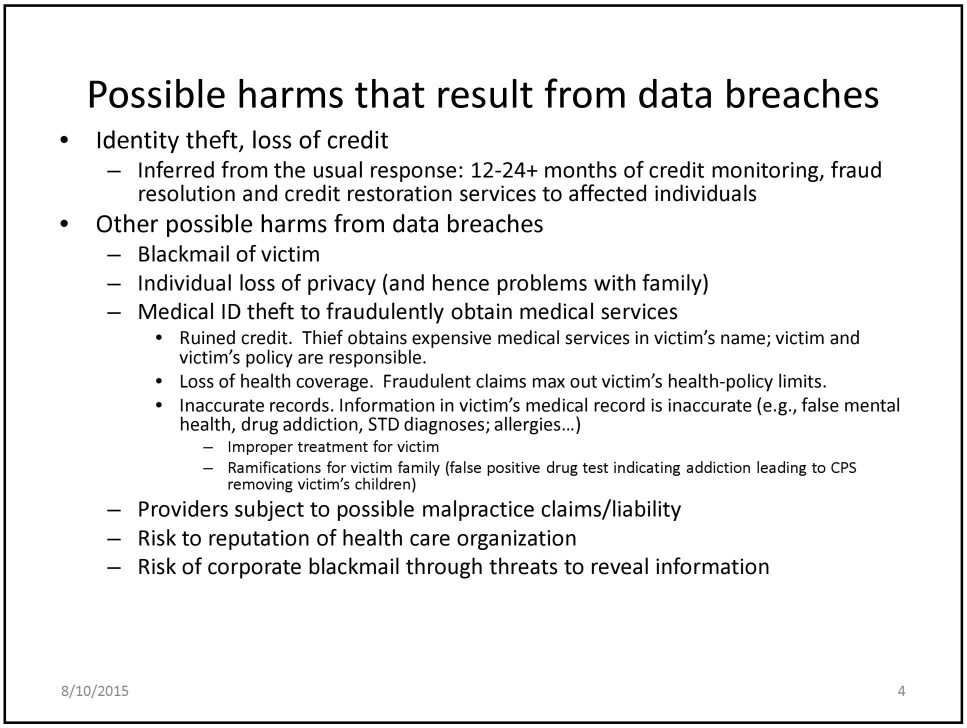
A very incomplete history of medical data breaches

Name	Date	Number of people affected	Type of incident	Ref
Anthem	3/15	79 M	Hacking/IT incident	(1)
SAIC	11/11	5 M	Loss (backup tapes)	(2)
Community Health Systems	8/14	4.5 M	Theft	(3)
UCLA	7/15	4.5 M	Hacking/IT incident	(4)
Medical Informatics Engineering	7/15	4 M	Hacking	(5)



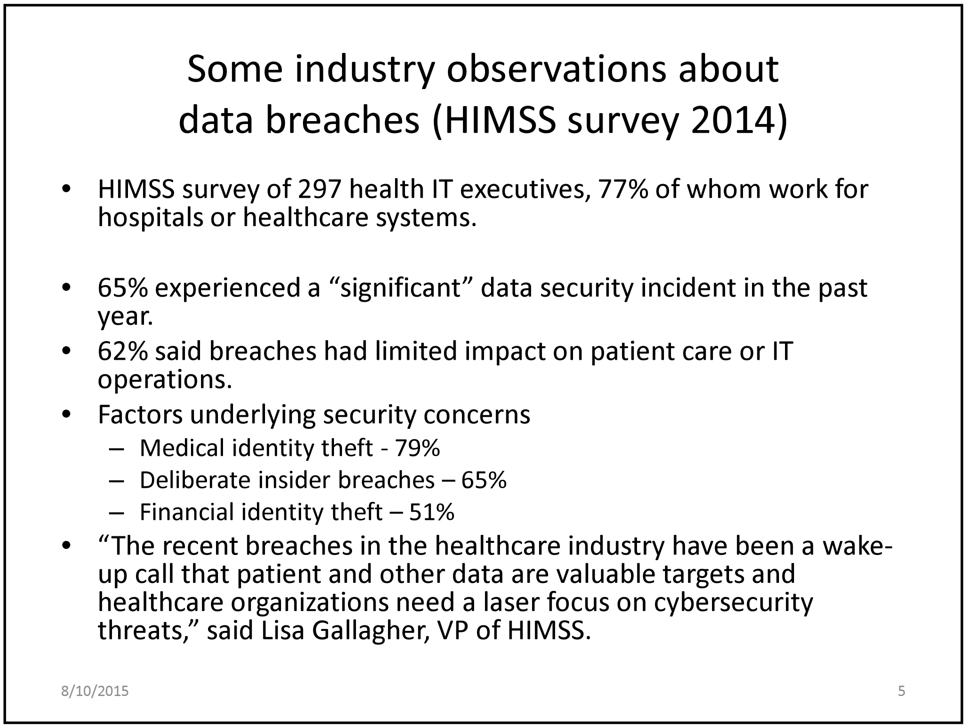
Advocate Medical Group	8/13	4 M	Theft of desktop computer	(6)
Xerox State Healthcare	9/14	2 M	Unauthorized access/disclosure	(7)
Health Net IBM	4/11	1.9 M	Loss of hard drives	(8)
GRM IMS	2/11	1.7 M	Theft of backup tapes	(9)
AvMed	6/10	1.2 M	Laptop with EMRs	(10)

All medical data breaches > 500 individuals since October 2009
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf



Possible harms that result from data breaches

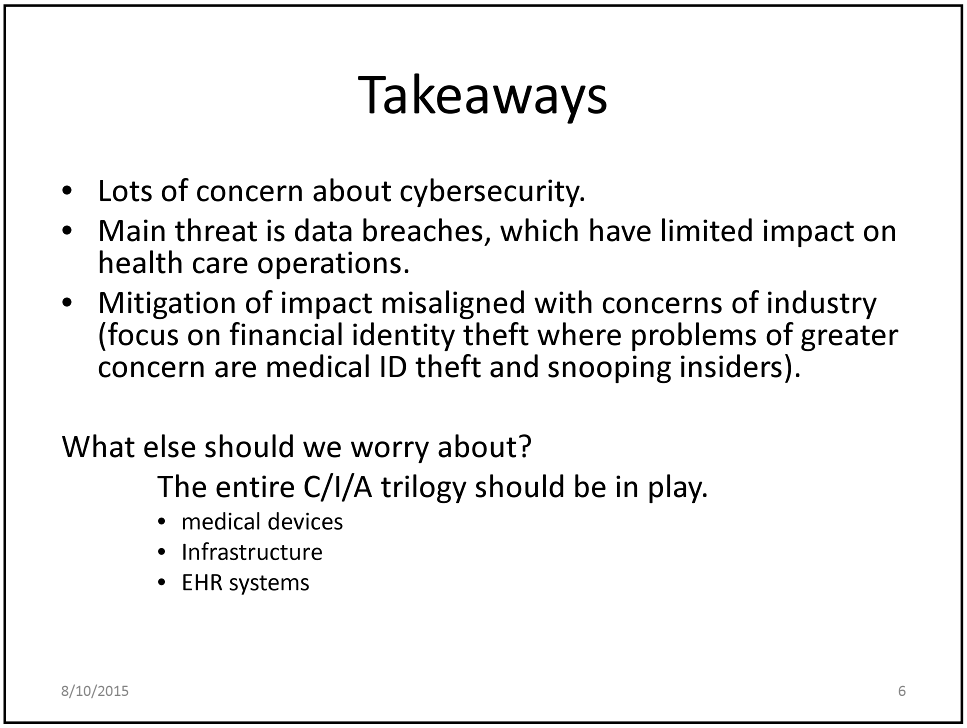
- Identity theft, loss of credit
  - Inferred from the usual response: 12-24+ months of credit monitoring, fraud resolution and credit restoration services to affected individuals
- Other possible harms from data breaches
  - Blackmail of victim
  - Individual loss of privacy (and hence problems with family)
  - Medical ID theft to fraudulently obtain medical services
    - Ruined credit. Thief obtains expensive medical services in victim's name; victim and victim's policy are responsible.
    - Loss of health coverage. Fraudulent claims max out victim's health-policy limits.
    - Inaccurate records. Information in victim's medical record is inaccurate (e.g., false mental health, drug addiction, STD diagnoses; allergies…)
      - Improper treatment for victim
      - Ramifications for victim family (false positive drug test indicating addiction leading to CPS removing victim's children)
  - Providers subject to possible malpractice claims/liability
  - Risk to reputation of health care organization
  - Risk of corporate blackmail through threats to reveal information



Some industry observations about data breaches (HIMSS survey 2014)

- HIMSS survey of 297 health IT executives, 77% of whom work for hospitals or healthcare systems.

- 65% experienced a “significant” data security incident in the past year.
- 62% said breaches had limited impact on patient care or IT operations.
- Factors underlying security concerns
  - Medical identity theft - 79%
  - Deliberate insider breaches – 65%
  - Financial identity theft – 51%
- “The recent breaches in the healthcare industry have been a wake-up call that patient and other data are valuable targets and healthcare organizations need a laser focus on cybersecurity threats,” said Lisa Gallagher, VP of HIMSS.



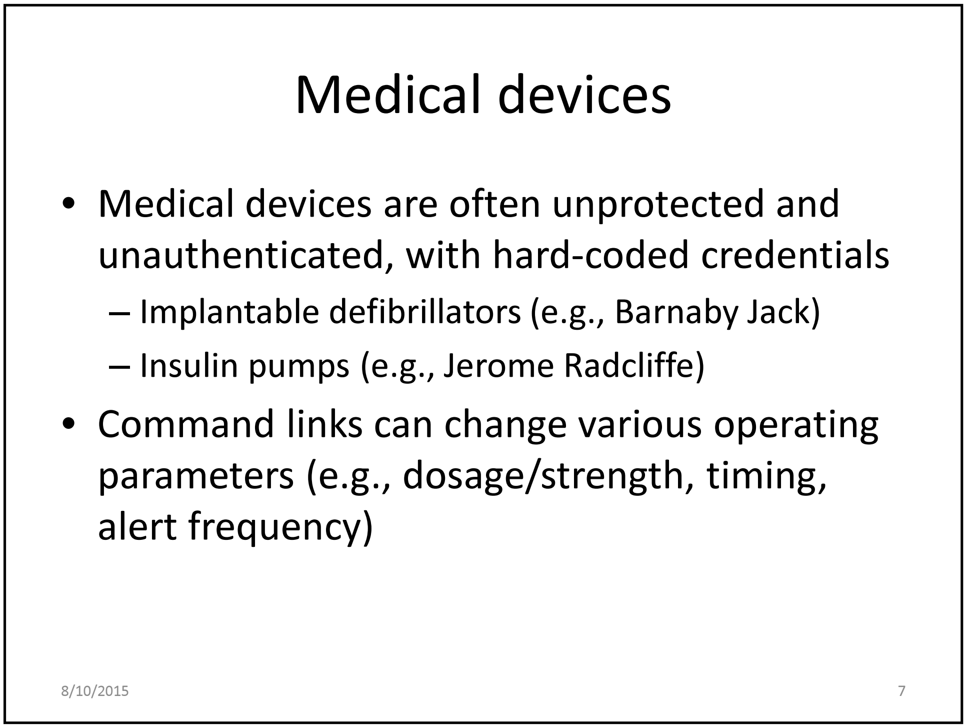
Takeaways

- Lots of concern about cybersecurity.
- Main threat is data breaches, which have limited impact on health care operations.
- Mitigation of impact misaligned with concerns of industry (focus on financial identity theft where problems of greater concern are medical ID theft and snooping insiders).

What else should we worry about?

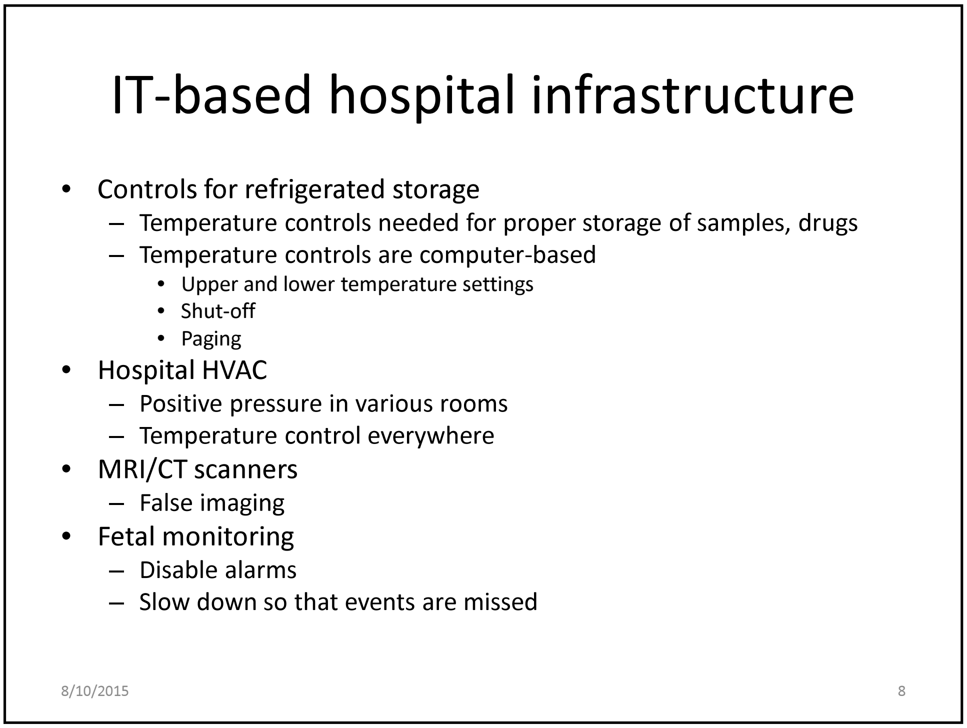
The entire C/I/A trilogy should be in play.

- medical devices
- Infrastructure
- EHR systems



Medical devices

- Medical devices are often unprotected and unauthenticated, with hard-coded credentials
  - – Implantable defibrillators (e.g., Barnaby Jack)
  - – Insulin pumps (e.g., Jerome Radcliffe)
- Command links can change various operating parameters (e.g., dosage/strength, timing, alert frequency)



IT-based hospital infrastructure

- Controls for refrigerated storage
  - – Temperature controls needed for proper storage of samples, drugs
  - – Temperature controls are computer-based
    - Upper and lower temperature settings
    - Shut-off
    - Paging
- Hospital HVAC
  - – Positive pressure in various rooms
  - – Temperature control everywhere
- MRI/CT scanners
  - – False imaging
- Fetal monitoring
  - – Disable alarms
  - – Slow down so that events are missed

EHR systems

- Denial of service
  - Shut down hospital servers; prevent access to electronic records
- Integrity
  - Alter correct medical information;
    - Bad diagnoses
  - Insert false/erroneous information;
    - Falsified medical records (mental health, STDs)
  - Cause bad orders to be given
    - Wrong dosages and types of medication
  - Change medical orders;

Types of threats to cybersecurity

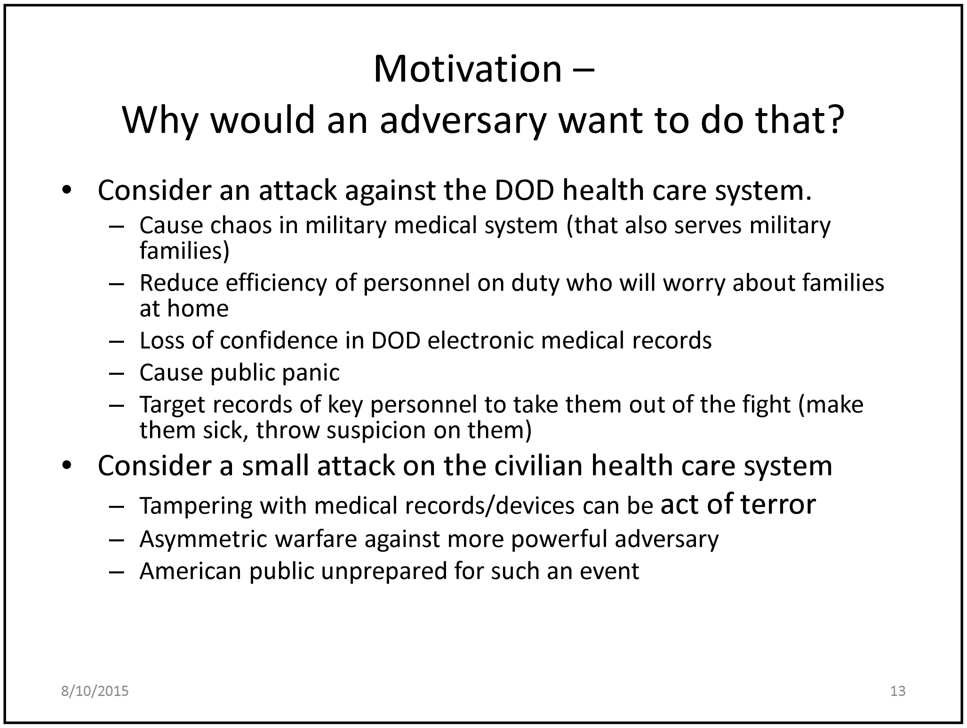
- Usual cyber threat to health information systems is exploitation – “cyberattack reveals private health information of Celebrity X”; “cyberattack exposes medical records of 10,000 people.”
- Usual bad guys:
  - Paparrazi in cyberspace
  - Celebrity chasers
  - Criminals (compromise medical information for blackmail/extortion; obtain resellable medical goods)
- Insurance companies (very rarely—they get their data legally)

A "new" type of threat

- Consider hostile operation that is genuinely an attack
  - Aimed at denying access or destroying or altering data or computer programs that store information or that run medical devices or instruments, EHR systems, health care infrastructure
  - Harms provision of care
  - Especially serious if coordinated with physical attack
- Smaller attack can harm public confidence in health care organizations or in entire system;
  - Sick people afraid to get medical care
  - Care providers afraid to rely on possibly-tainted records (but still probably accurate)

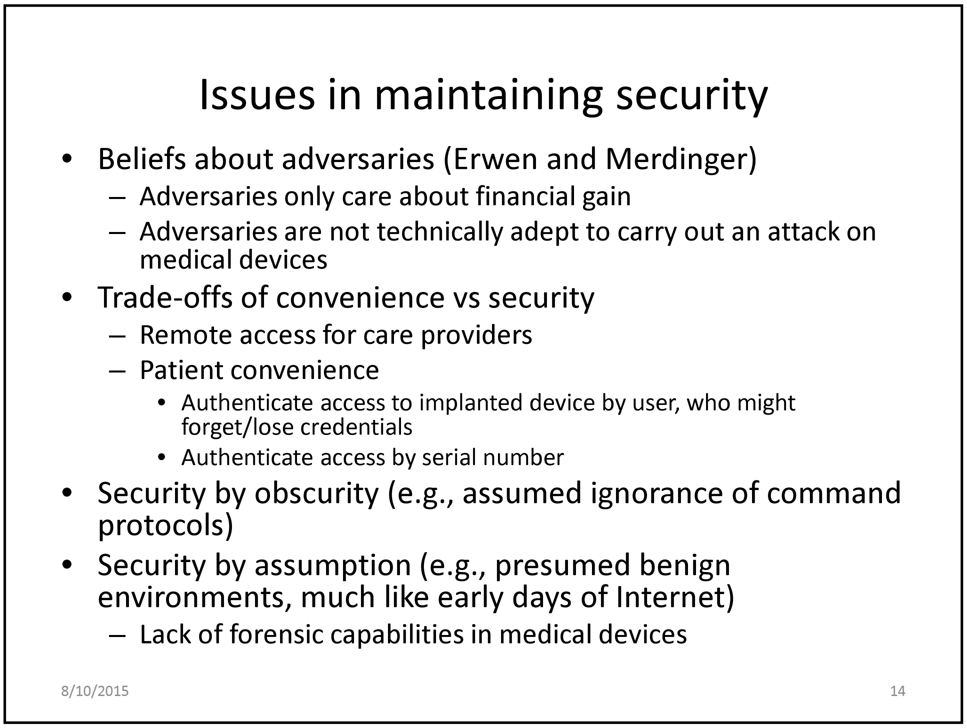
New potential adversaries…

- Individuals
  - Those seeking to do harm to individual patients
    - Personal motivations
    - Political ("cause") motivations
  - Those seeking to harm care providers (e.g., thru malpractice lawsuits)
    - Change providers of record to change compensation
    - change billing so that Doc X is recorded as MD of record when Doc Y did all the work…
  - Patients themselves (e.g., drug addicts)
- Competitor care-providing organizations
- Terrorist groups
- Adversary nation states
  - Resources available are much larger
  - Money, time, hacker talent
  - Intelligence services available (imagine agency-scale resources trying to penetrate electronic medical records system of a hospital – no contest)



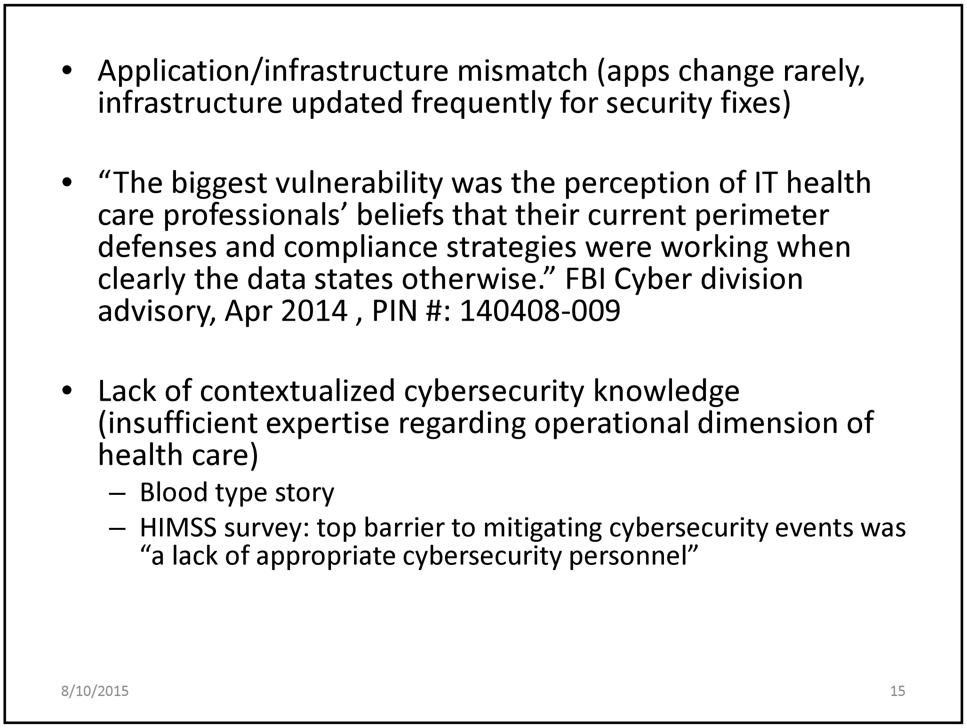
Motivation – Why would an adversary want to do that?

- Consider an attack against the DOD health care system.
  - – Cause chaos in military medical system (that also serves military families)
  - – Reduce efficiency of personnel on duty who will worry about families at home
  - – Loss of confidence in DOD electronic medical records
  - – Cause public panic
  - – Target records of key personnel to take them out of the fight (make them sick, throw suspicion on them)
- Consider a small attack on the civilian health care system
  - – Tampering with medical records/devices can be act of terror
  - – Asymmetric warfare against more powerful adversary
  - – American public unprepared for such an event



Issues in maintaining security

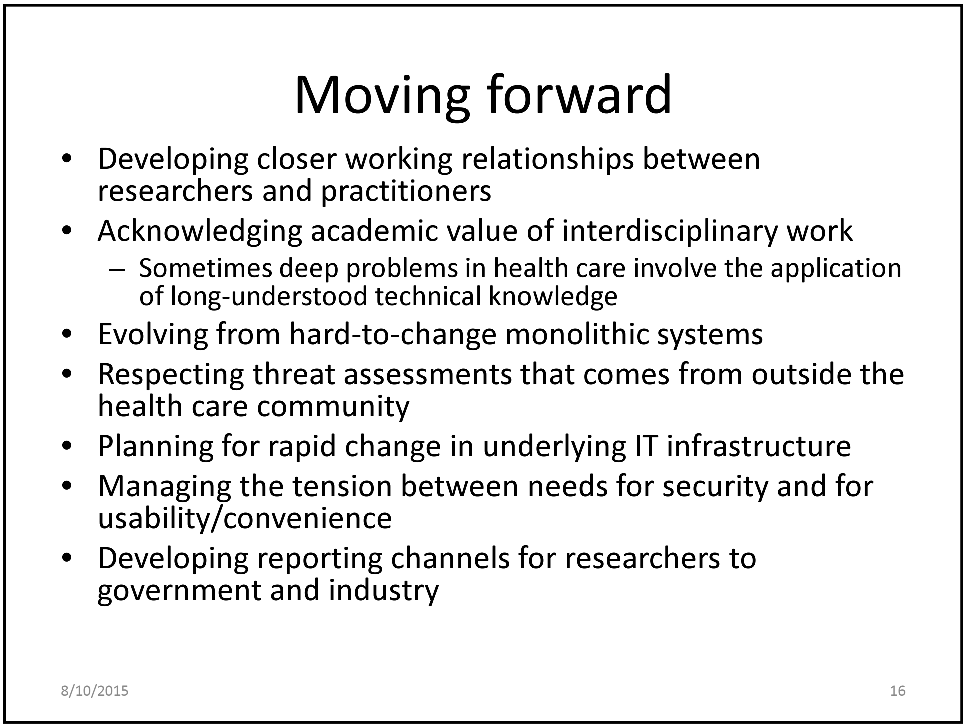
- Beliefs about adversaries (Erwen and Merdinger)
  - – Adversaries only care about financial gain
  - – Adversaries are not technically adept to carry out an attack on medical devices
- Trade-offs of convenience vs security
  - – Remote access for care providers
  - – Patient convenience
    - Authenticate access to implanted device by user, who might forget/lose credentials
    - Authenticate access by serial number
- Security by obscurity (e.g., assumed ignorance of command protocols)
- Security by assumption (e.g., presumed benign environments, much like early days of Internet)
  - – Lack of forensic capabilities in medical devices



- Application/infrastructure mismatch (apps change rarely, infrastructure updated frequently for security fixes)

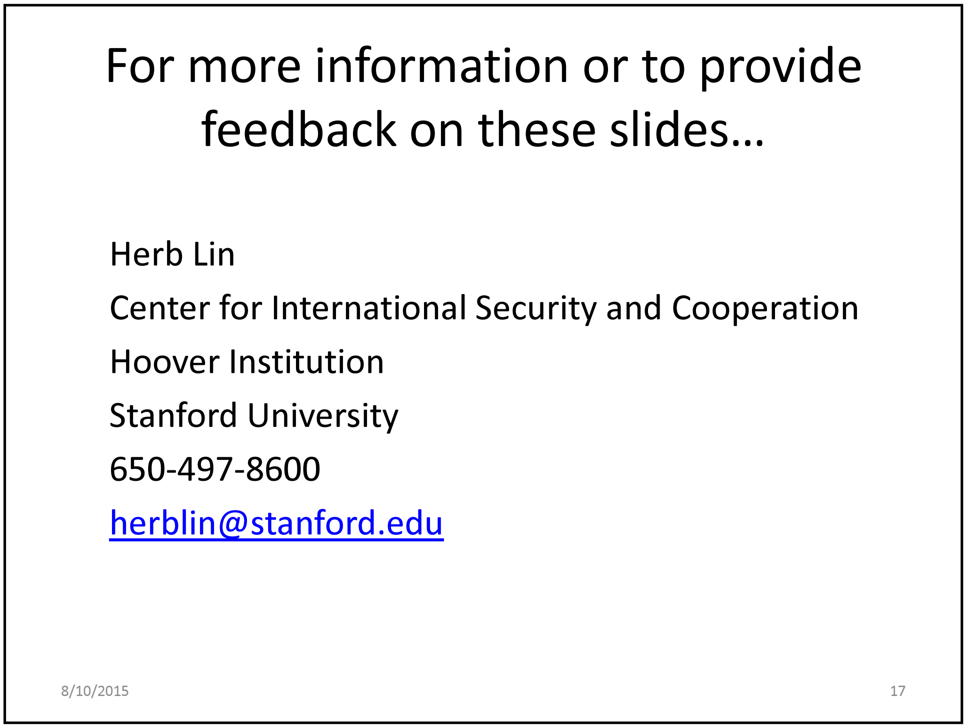
- "The biggest vulnerability was the perception of IT health care professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise." FBI Cyber division advisory, Apr 2014 , PIN #: 140408-009

- Lack of contextualized cybersecurity knowledge (insufficient expertise regarding operational dimension of health care)
  - Blood type story
  - HIMSS survey: top barrier to mitigating cybersecurity events was "a lack of appropriate cybersecurity personnel"



Moving forward

- Developing closer working relationships between researchers and practitioners
- Acknowledging academic value of interdisciplinary work
  - Sometimes deep problems in health care involve the application of long-understood technical knowledge
- Evolving from hard-to-change monolithic systems
- Respecting threat assessments that comes from outside the health care community
- Planning for rapid change in underlying IT infrastructure
- Managing the tension between needs for security and for usability/convenience
- Developing reporting channels for researchers to government and industry



For more information or to provide feedback on these slides…

Herb Lin
Center for International Security and Cooperation
Hoover Institution
Stanford University
650-497-8600
herblin@stanford.edu

8/10/2015 17