SCCE NY REGIONAL CONFERENCE
MAY 15, 2015
JANET K. HIMMELREICH, *CCEP, CCEP-I, CIPP/US*

You can have Security Without Privacy but
You can't have Privacy without Security

OVERVIEW

- Privacy vs Security – Discussion
- Cybersecurity Imperatives
- Examining a few scenarios and case studies
- Impacts to your Compliance team
- 5 Things to do when you get back to work

WHO WE ARE ***NOT*** TALKING ABOUT TODAY

But, you really can't have a discussion like this without at least acknowledging Edward Snowden's impact on the way we think about Privacy and Security

YOU CAN HAVE SECURITY WITHOUT PRIVACY BUT YOU CAN'T HAVE PRIVACY WITHOUT SECURITY

What does that mean in a practical sense?

PRIVACY VS SECURITY

PRIVACY

the state or condition of being free from being observed or disturbed by other people.

While say Google's servers are secured from data breaches, what is to stop someone from reading your emails? This is the essence of privacy

SECURITY

the state of being free from danger or threat.

Includes technological solutions to protect from data theft and breach; ID badges for physical security; solutions are commonly known

Definitions per Privacy vs. Security:
The Important Difference
By KCnext on September 5, 2013

5

CONCEPTUAL FRAMEWORK

- Process or action
- Condition
- Strategy
- State of existence
- Tactical
- Sealed envelope

- Result
- Prognosis
- Outcome
- Supporting evidence
- Strategic objective
- Message inside successfully delivered

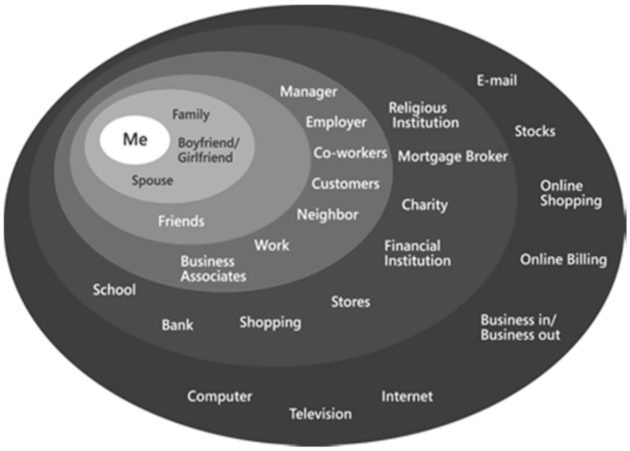
Security	**Privacy**

6

PRIVACY BASICS

SHARING PERSONAL INFORMATION

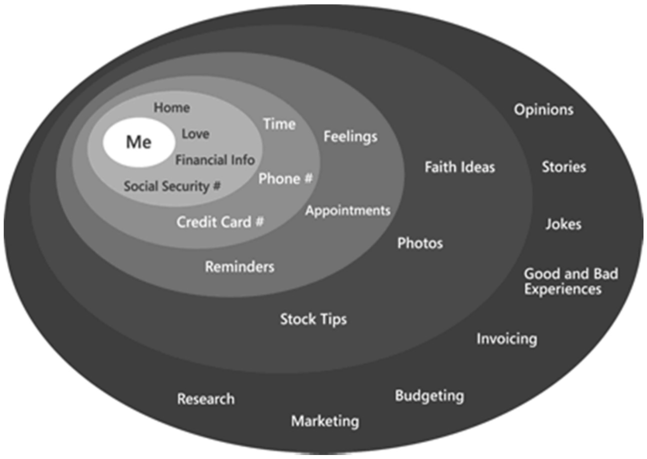
The further away, the less willing the person is to share information



Microsoft 2003

INFORMATION USERS FEEL COMFORTABLE SHARING

The further the item, the more comfortable sharing



Microsoft 2003

ADEQUATE PROCEDURES

- Privacy Notices – (term “policies” frequently incorrectly used) – interface to your customer
  - If you tell them you will protect their personal information (as defined by you), you’d better do it!
  - Requires:
    - Training
    - Written procedures
    - Notification processes
    - Management oversight
    - Communication, communication, communication

ACROSS INDUSTRIES

- Chief Privacy Officer (or similar)
- Privacy Plans
  - Establishes the parameters your company will use around often conflicting and overlapping global regulations
  - Defines what data will be protected
  - Defines the “need to know” concept for the various types of data or information in your custody
  - Expedites requests for information
    - From consumer or patient
    - From third parties or other partners
    - From regulators
  - Audit readiness

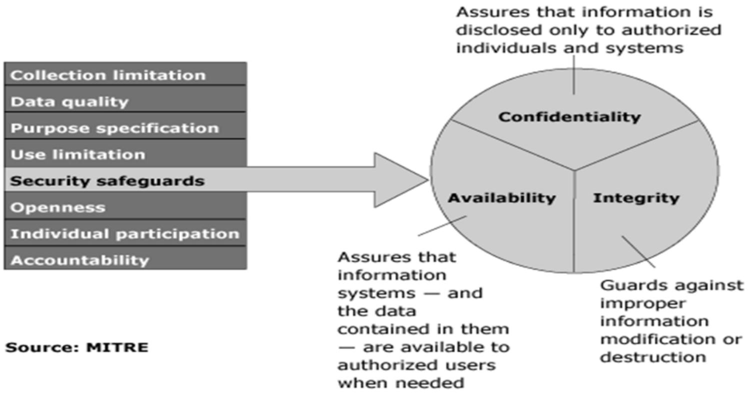
SECURITY BASICS

If only you could just click a button!

SECURITY PLAN ATTRIBUTES

CIA

Safeguards

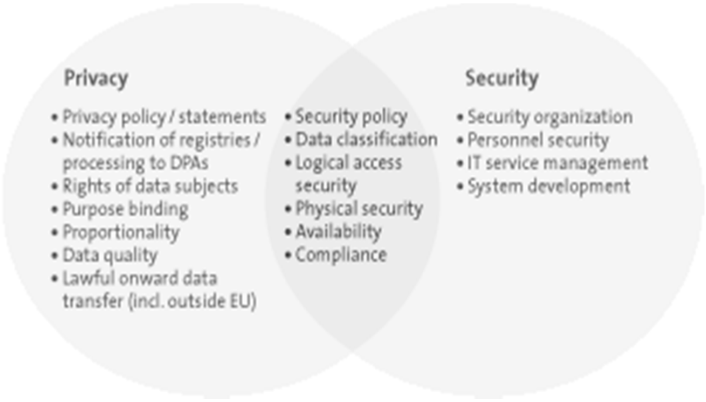

Assures that information is disclosed only to authorized individuals and systems
Collection limitation
Data quality
Purpose specification
Use limitation
Security safeguards
Openness
Individual participation
Accountability
Confidentiality
Availability
Integrity
Assures that information systems — and the data contained in them — are available to authorized users when needed
Guards against improper information modification or destruction

Source: MITRE

SAFEGUARDS

- Policies, processes and tools required to maintain the privacy and confidentiality promised by the Privacy warrants
- Scope is greater than just technology
- Methods, training, processes, monitoring and reporting
- Prevention of breaches but if one occurs, managing the breach for least impact
- Chief Information Security Officer (CISO, SO, SCO…)

THEY OVERLAP



Privacy

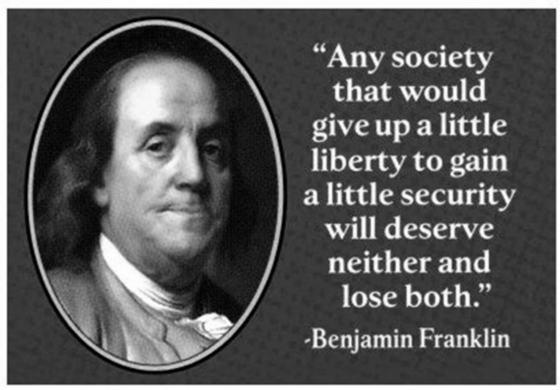
- Privacy policy / statements
- Notification of registries / processing to DPAs
- Rights of data subjects
- Purpose binding
- Proportionality
- Data quality
- Lawful onward data transfer (incl. outside EU)

- Security policy
- Data classification
- Logical access security
- Physical security
- Availability
- Compliance

Security

- Security organization
- Personnel security
- IT service management
- System development

Source: Ronald Koorn and Joris ter Hart IT Advisory KPMG, NL Feb. 2011


"Any society that would give up a little liberty to gain a little security will deserve neither and lose both."
-Benjamin Franklin

CYBERSECURITY IN THE HEADLINES

- Sony, Anthem, Jennifer Lawrence, Target, Home Depot, the White House…….
- China, Russia, North Korea, the Mafia, high school kids, NSA……….
- Millions in fines and penalties
- Impacts to stock value
- Brand reputation damage

SHORT DEFINITIONS

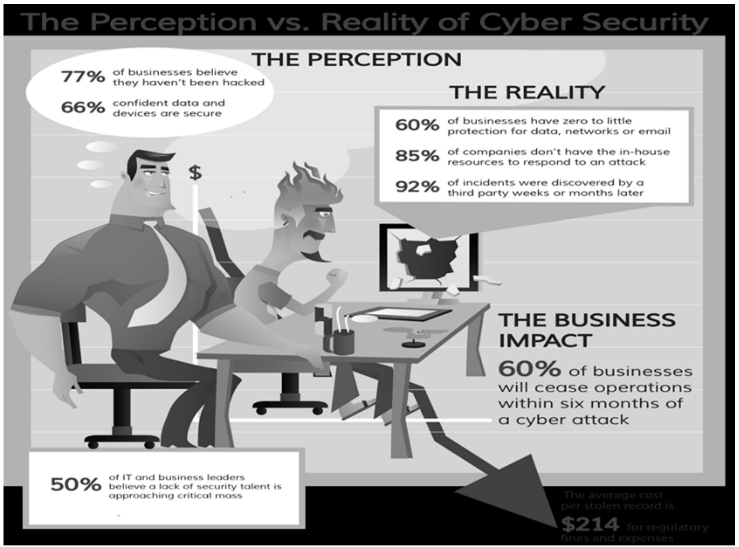
- Cybersecurity*:*
  - measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack
  - **First Known Use of term:** 1994
- Cyberspace:
  - The interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Merriam Webster Dictionary; Adapted from: NSPD 54/HSPD -23, CNSSI 4009, NIST SP 800-53 Rev 4

A MORE EXPANDED VIEW

- Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
- Extended Definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009



The Perception vs. Reality of Cyber Security

THE PERCEPTION

77% of businesses believe they haven't been hacked

66% confident data and devices are secure

THE REALITY

60% of businesses have zero to little protection for data, networks or email

85% of companies don't have the in-house resources to respond to an attack

92% of incidents were discovered by a third party weeks or months later

THE BUSINESS IMPACT

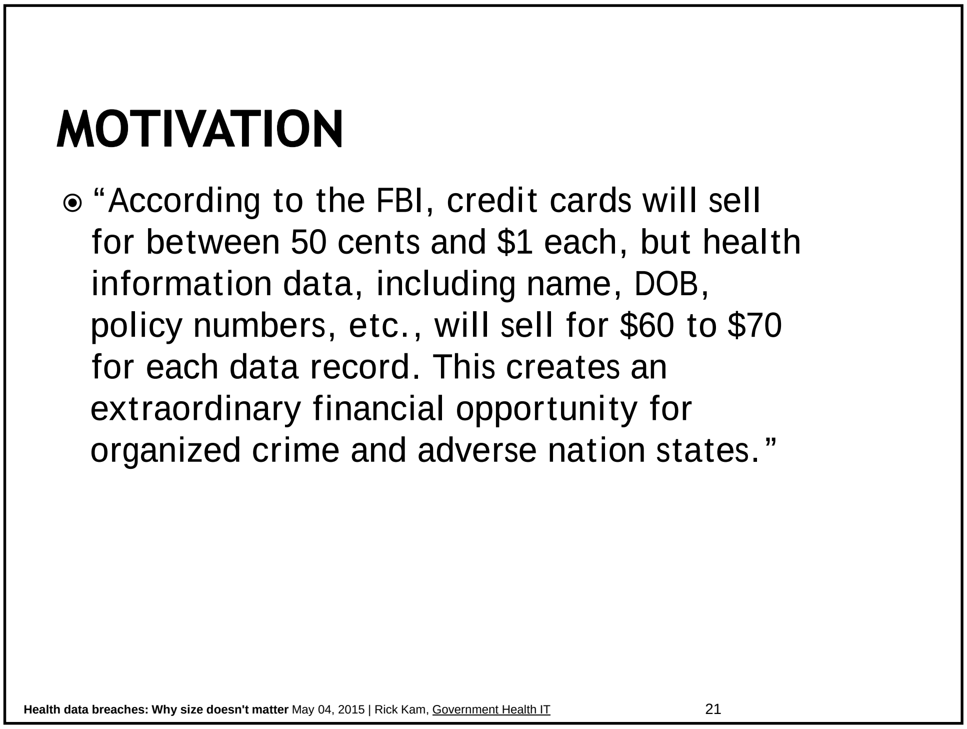
60% of businesses will cease operations within six months of a cyber attack

50% of IT and business leaders believe a lack of security talent is approaching critical mass

The average cost per stolen record is $214 for regulatory fines and expenses

The average cost per stolen record in Regulatory fines and expenses

Updated Infographic: The Perception vs. Reality of Cyber Security Wolf Networks is an IT service provider.
by Martin (Arctic Wolf) on Mar 24, 2014 at 12:28 PM



MOTIVATION

- “According to the FBI, credit cards will sell for between 50 cents and $1 each, but health information data, including name, DOB, policy numbers, etc., will sell for $60 to $70 for each data record. This creates an extraordinary financial opportunity for organized crime and adverse nation states.”

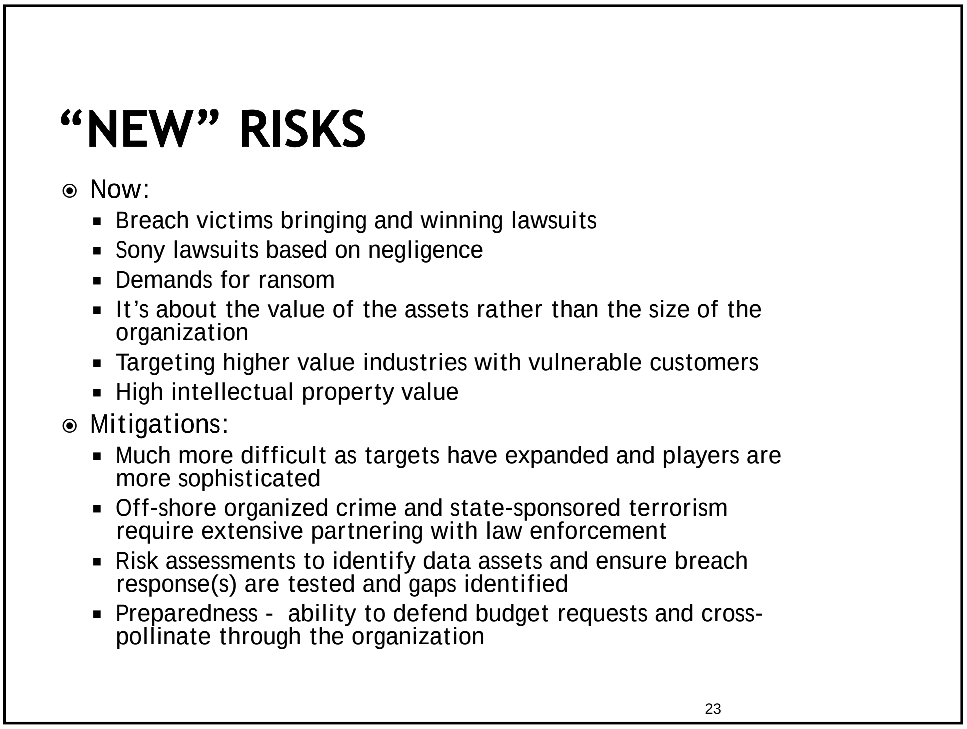
Health data breaches: Why size doesn't matter May 04, 2015 | Rick Kam, Government Health IT

21

“OLD” RISKS

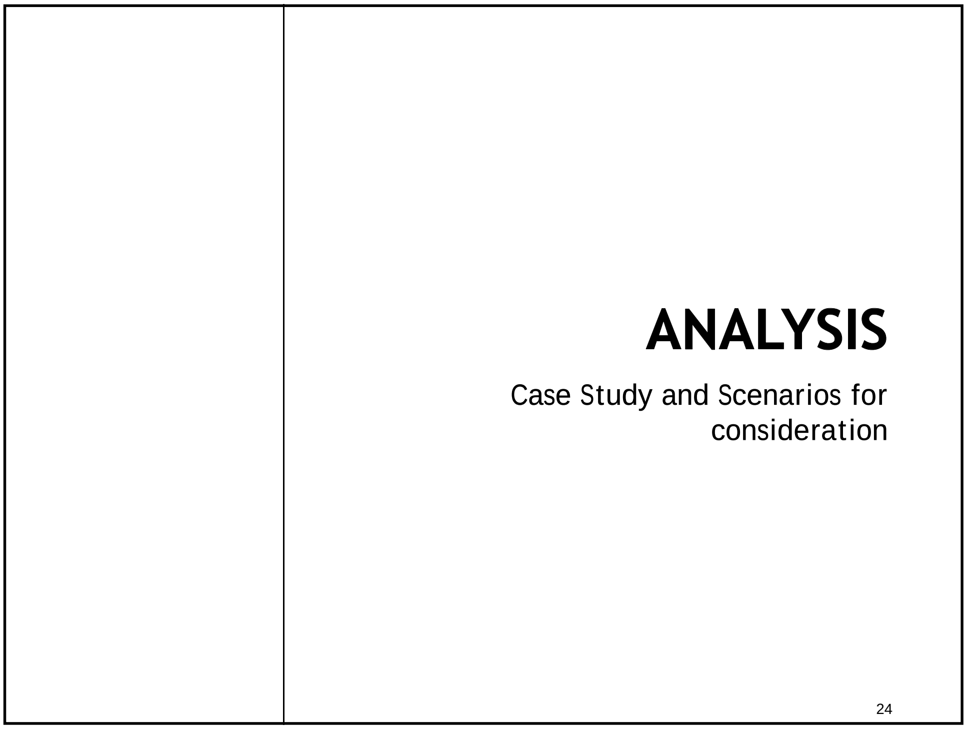
- Conventional wisdom:
  - Identity theft
  - Lost business
  - Possible regulatory fines
- Mitigations:
  - Report it if breach big enough to meet regulatory requirements
  - Set up free credit monitoring
  - Good PR campaign

22



“NEW” RISKS

- Now:
  - Breach victims bringing and winning lawsuits
  - Sony lawsuits based on negligence
  - Demands for ransom
  - It’s about the value of the assets rather than the size of the organization
  - Targeting higher value industries with vulnerable customers
  - High intellectual property value
- Mitigations:
  - Much more difficult as targets have expanded and players are more sophisticated
  - Off-shore organized crime and state-sponsored terrorism require extensive partnering with law enforcement
  - Risk assessments to identify data assets and ensure breach response(s) are tested and gaps identified
  - Preparedness - ability to defend budget requests and cross-pollinate through the organization



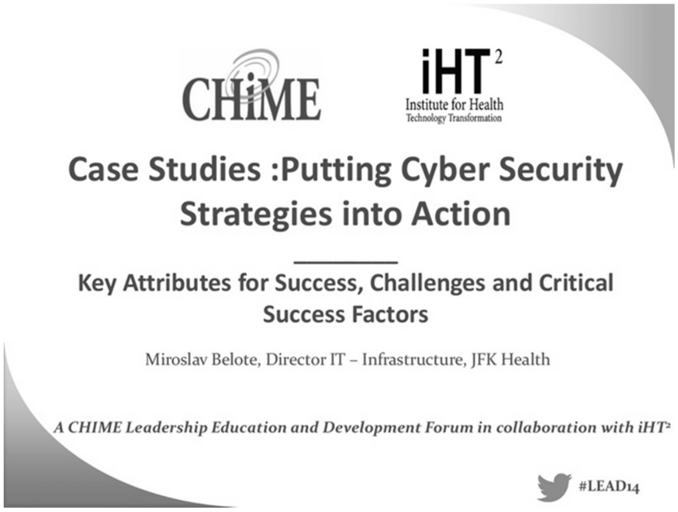
ANALYSIS

Case Study and Scenarios for consideration

SCENARIOS – PRIVACY OR SECURITY ISSUE?

- A large consumer products company mails baby-related coupons to a teenager who's family didn't know she was pregnant. Is that a privacy or security violation?
- A large bank sends it's customers an annual description of their privacy practices with regard to the customer information that they collect and hold on to as part of their operations. They pass some of that information on to a mortgage company that has a totally different name than the bank but is a subsidiary company. Is that a privacy or security violation?
- For more than six months in late 2013 and early 2014, employees of Mexico, Columbia and the Philippines call centers, with systems maintained and operated by a large teleco and subject to the company's data security practices, used their login credentials to access customer's accounts and grab the names and last four digits of Social Security numbers. The personal information that employees had taken without authorization was used by mafia gangs to submit 290,000 handset unlock requests for mobile phones through the teleco provider's website. Is that a privacy or a security violation?

CASE STUDY – CYBER-SECURITY IN HEALTHCARE


CHiME
iHT²
Institute for Health Technology Transformation

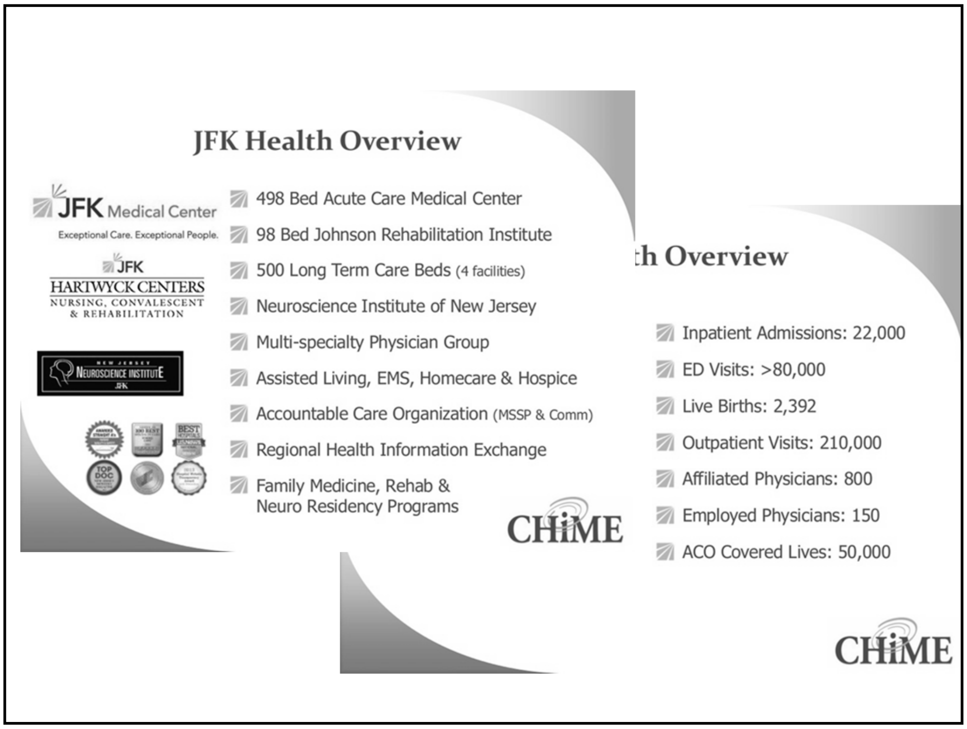
Case Studies :Putting Cyber Security Strategies into Action

Key Attributes for Success, Challenges and Critical Success Factors

Miroslav Belote, Director IT – Infrastructure, JFK Health

A CHIME Leadership Education and Development Forum in collaboration with iHT²

#LEAD14

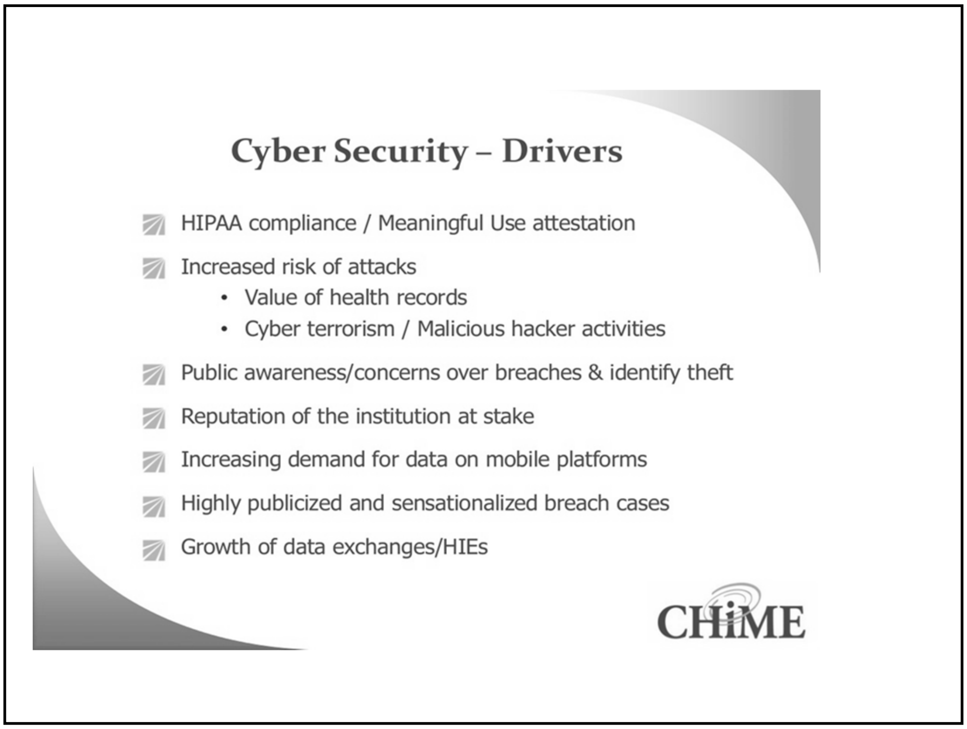

JFK Medical Center
Exceptional Care. Exceptional People.
JFK
HARTWYCK CENTERS
NURSING, CONVALESCENT & REHABILITATION
NEW JERSEY NEUROSCIENCE INSTITUTE
JFK
CHiME
CHiME

JFK Health Overview

- 498 Bed Acute Care Medical Center
- 98 Bed Johnson Rehabilitation Institute
- 500 Long Term Care Beds (4 facilities)
- Neuroscience Institute of New Jersey
- Multi-specialty Physician Group
- Assisted Living, EMS, Homecare & Hospice
- Accountable Care Organization (MSSP & Comm)
- Regional Health Information Exchange
- Family Medicine, Rehab & Neuro Residency Programs

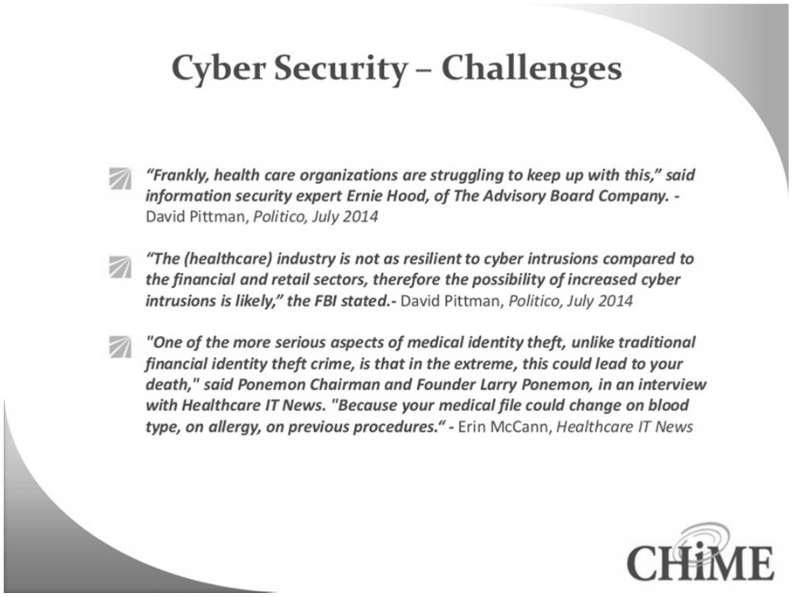
th Overview

- Inpatient Admissions: 22,000
- ED Visits: >80,000
- Live Births: 2,392
- Outpatient Visits: 210,000
- Affiliated Physicians: 800
- Employed Physicians: 150
- ACO Covered Lives: 50,000



Cyber Security – Drivers

- HIPAA compliance / Meaningful Use attestation
- Increased risk of attacks
  - Value of health records
  - Cyber terrorism / Malicious hacker activities
- Public awareness/concerns over breaches & identify theft
- Reputation of the institution at stake
- Increasing demand for data on mobile platforms
- Highly publicized and sensationalized breach cases
- Growth of data exchanges/HIEs



Cyber Security – Challenges

- *"Frankly, health care organizations are struggling to keep up with this," said information security expert Ernie Hood, of The Advisory Board Company.* - David Pittman, *Politico, July 2014*
- *"The (healthcare) industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely," the FBI stated.*- David Pittman, *Politico, July 2014*
- *"One of the more serious aspects of medical identity theft, unlike traditional financial identity theft crime, is that in the extreme, this could lead to your death," said Ponemon Chairman and Founder Larry Ponemon, in an interview with Healthcare IT News. "Because your medical file could change on blood type, on allergy, on previous procedures."* - Erin McCann, *Healthcare IT News*

CHiME

IMPACTS TO YOUR COMPLIANCE TEAM

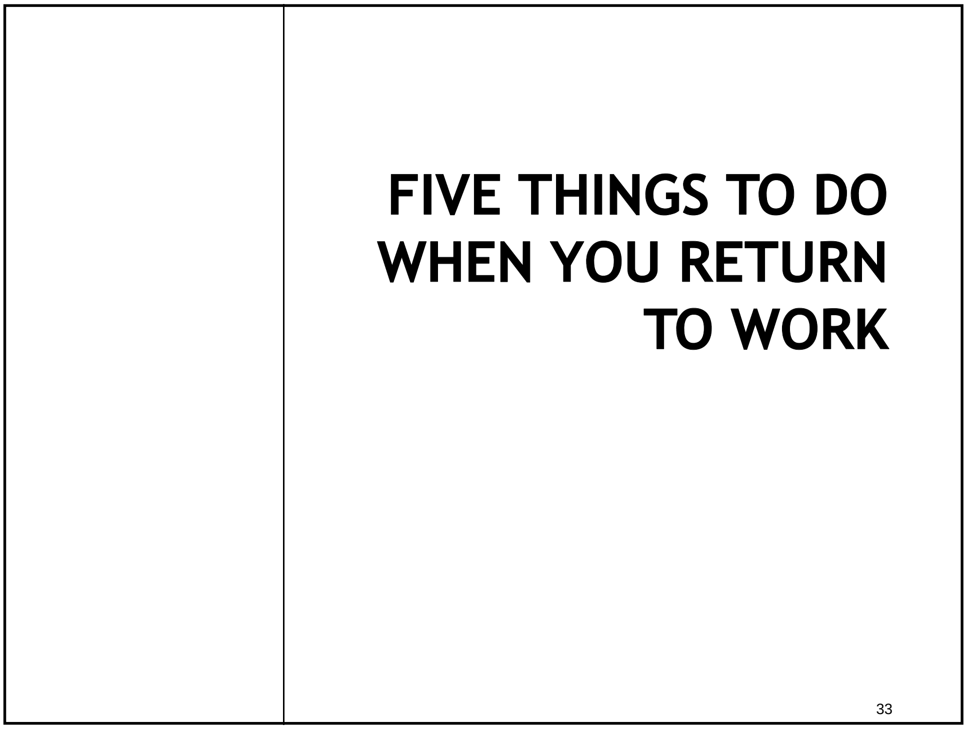
30

IMPACTS

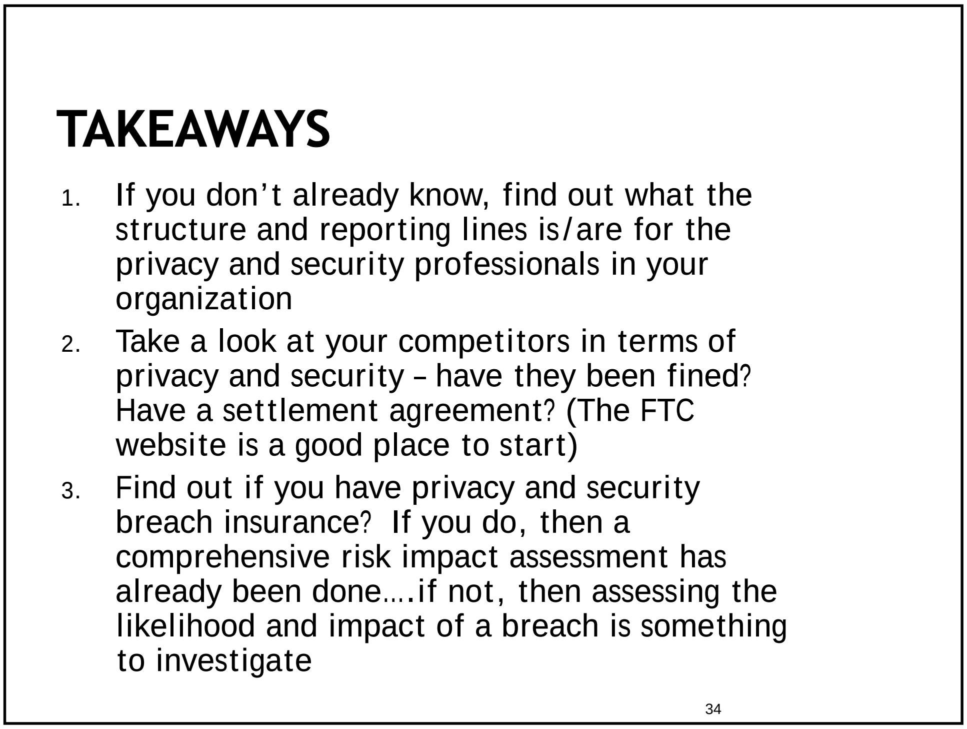
- All programs are under pressure to reduce costs and to show return on investment
  - Encompassing or partnering around privacy requirements is one way to enhance the Compliance Team’s scope/value
  - Risks around non-compliance to Privacy requirements and employing “adequate” safeguards are increasing daily; what was in place even a year or two ago is probably not proportionate to the current risk
  - Regulatory enforcement is increasing as are the fines and penalties associated with it
  - Lawsuits are now recognized as one way to manage the effect of a breach
- The FCC just mandated that AT&T employ a formally trained and certified Privacy Compliance Officer – other regulatory agencies are likely to follow this lead
- Do you know what your marketing department is doing with all that data?

MORE QUESTIONS

- Have you been hacked? (statistics say that you most likely have been)
- Do you have a separate Privacy and/or Security Program?
  - Where is the responsibility for Privacy in your organization?
  - Where is Security? Physical Security, Information Security, Employee Security…..
  - If Privacy is a separate function – how are you aligned?
  - If it is part of the overall Compliance function then is it given proper attention and importance?
- Where does your Board stand relative to Privacy and Security?
- If you have a Privacy Notice or Policy on your website – do YOU know how it is being implemented and enforced?

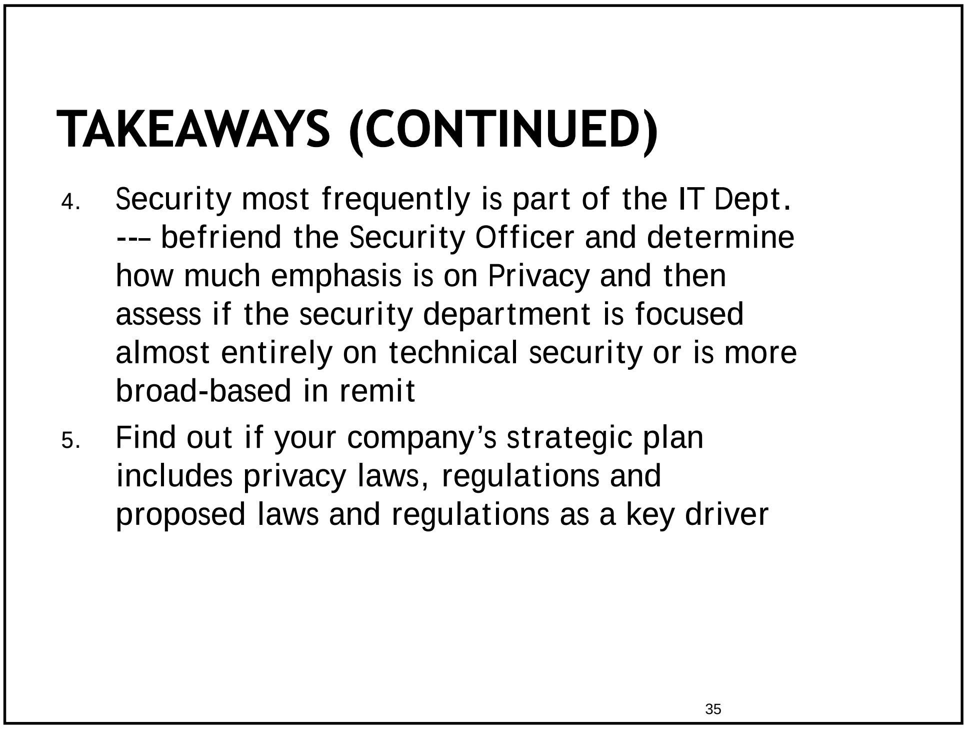


FIVE THINGS TO DO WHEN YOU RETURN TO WORK



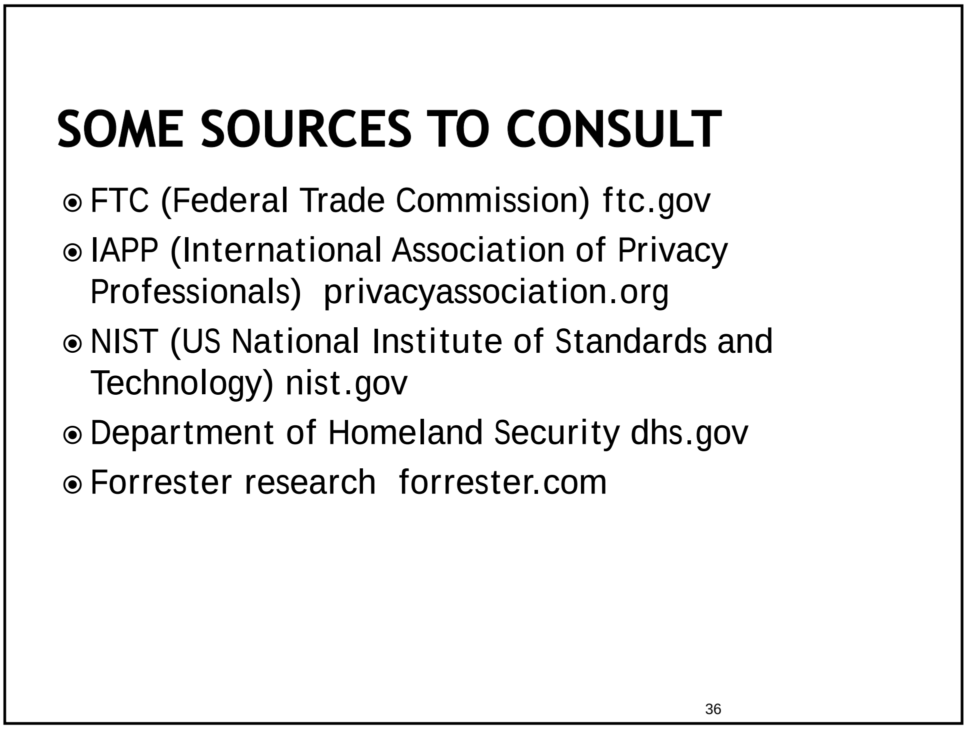
TAKEAWAYS

1. If you don’t already know, find out what the structure and reporting lines is/are for the privacy and security professionals in your organization
2. Take a look at your competitors in terms of privacy and security – have they been fined? Have a settlement agreement? (The FTC website is a good place to start)
3. Find out if you have privacy and security breach insurance? If you do, then a comprehensive risk impact assessment has already been done….if not, then assessing the likelihood and impact of a breach is something to investigate



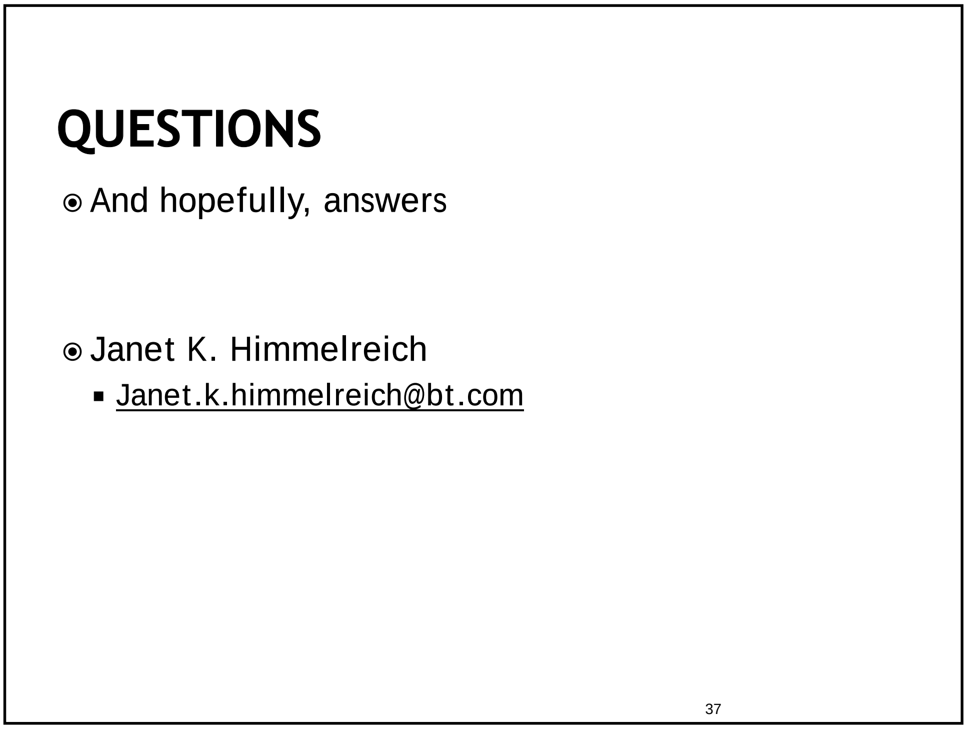
TAKEAWAYS (CONTINUED)

4. Security most frequently is part of the IT Dept. --– befriend the Security Officer and determine how much emphasis is on Privacy and then assess if the security department is focused almost entirely on technical security or is more broad-based in remit
5. Find out if your company’s strategic plan includes privacy laws, regulations and proposed laws and regulations as a key driver



SOME SOURCES TO CONSULT

- FTC (Federal Trade Commission) ftc.gov
- IAPP (International Association of Privacy Professionals) privacyassociation.org
- NIST (US National Institute of Standards and Technology) nist.gov
- Department of Homeland Security dhs.gov
- Forrester research forrester.com



QUESTIONS

- And hopefully, answers

- Janet K. Himmelreich
  - Janet.k.himmelreich@bt.com