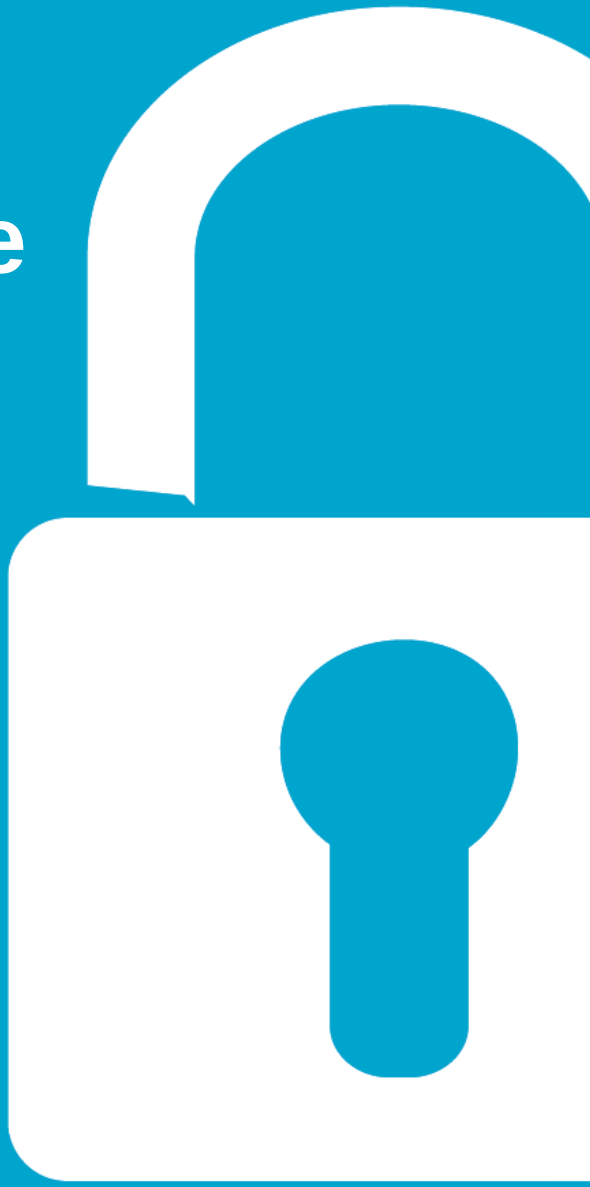
5th Annual Montana HIMSS Spring Convention and Tradeshow

Adopting a Cybersecurity Framework for Governance and Risk Management

Jim Hunter

Director, Monitoring and Security

CareTech Solutions



Learning Objectives

1. Identify current healthcare privacy and cybersecurity threats and risks

2. Assess the readiness of healthcare providers, business associates, leadership and trustees to respond to current cybersecurity threats

3. Explain the role of the board in managing cybersecurity risks in the context of enterprise risk management

4. Explain the value of a cybersecurity framework for healthcare and hospital governance and enterprise risk management

LOS ANGELES TIMES

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

The Hollywood Presbyterian Medical Center. The hospital was recently the target of a ransomware extortion plot in which hackers seized control its computer systems and then demanded that directors pay in bitcoin to regain access[1]
(Ricardo DeAratanha / Los Angeles Times)

Ransomware in the headlines

In the wake of Hollywood Presbyterian, several other hospitals and health systems were attacked:

- Chino Valley Medical Center and Desert Valley Hospital of Prime Healthcare were hit the same week as Methodist Hospital in Kentucky and Ottawa Hospital in Ottawa Canada[1]

- MedStar Health, a chain of 10 hospitals in the Washington, D.C. area, had their computers hit and had to run on paper for one week![2]

1 *Monegain, Bernie. "Hackers hit two California hospitals with ransomware." Healthcare IT News. Mar. 3, 2016. Web. Apr. 27, 2016. http://healthcareitnews.com/news/hackers-hit-two-california-hospitals-ransomware.*

2 *Murphy, PhD, Kyle, "Ransomware Leads to EHR Downtime at DC-Area Health System." EHR Intelligence. Mar. 29, 2016. Web. Apr. 27, 2016. https://ehrintelligence.com/news/ransomware-leads-to-ehr-downtime-at-dc-area-health-system*

2015: The Rise of Criminal Attacks on Healthcare Data

"…for the first time, criminal attacks are the number-one cause of healthcare data breaches."

Criminal attacks on healthcare organizations are up **125%** compared to 5 years ago. In fact, **45%** of healthcare organizations say the root cause of the data breach was a criminal attack, and **12%** say it was due to a malicious insider.

Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Sponsored by ID Experts
Independently conducted by Ponemon Institute LLC, May 2015

Healthcare Data Breaches Are Costly

- **90%** had a data breach in the past 2 years, **40%** had more than 5
- Average economic impact due to data breaches is **2.1 million dollars** / healthcare organization and **1 million dollars** / business associate organizations over 2 years
- Criminal attacks are now the **#1 cause** of data breaches
- **56%** of healthcare organizations and **59%** of business associates don't believe their incident response process has adequate funding and resources

FBI Cyber Division: Private Industry Notification


UNCLASSIFIED

FBI CYBER DIVISION

Private Industry Notification

(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain

17 April 2014

Cyber actors will likely increase cyber intrusions again health care systems—to include medical devices—due to…

- Mandatory transition from paper to electronic health records (EHR)
- Lax cybersecurity standards
- A higher financial payout for medical records in the black market

The healthcare industry is not technically prepared to combat cybercriminals basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)

What Makes Healthcare Data So Valuable to Cybercriminals?

- Healthcare records are a rich set of data:
  - Financial, medical, family, and personal data
- Healthcare data can be used to:
  - Obtain healthcare services, drugs or medical devices
  - Insurance fraud
  - Financial fraud (open financial accounts)
- A healthcare record can be worth $50 to $1,000
  - Credit card data typically sells for $1 each
- Healthcare fraud detection is poor

Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015, PwC

What Makes Healthcare Data So Valuable to Cybercriminals?

- Data has a variety of other uses:
  - Election year! Obtain personal information for extortion, bad publicity or even worst intentions
    - Prescriptions taking
    - Medical conditions
    - Overall health
  - Terrorist activities
    - Medical device tampering
    - Drug interactions
  - Ransomware can hold data hostage and interrupt care delivery until either the ransom is paid or backups restore data

Recent Breaches & Settlement Agreements

CareFirst BlueCross BlueShield

May 20, 2015

1,100,000

CHS Community Health Systems, Inc.

August 18, 2014

4,500,000

UCLA Health

May 5, 2015

4,500,000

mie Medical Informatics Engineering

June 10, 2015

Unknown

Premera Blue Cross

March 17, 2015

11,000,000

Anthem BlueCross

March 15, 2015

78, 800,000

patient records

- Breaches due to hackers
- Anthem is the largest healthcare data breach in US history
- Medical Informatics Engineering is an EMR vendor with some very large customers

Recent Breaches & Settlement Agreements

Santa Rosa Memorial Hospital – St. Joseph Health System

June 14, 2014

34,000

Est. cost: $13.5M

- SRMH: Stolen unencrypted USB drive
- Concentra: Stolen unencrypted laptop

Concentra®

November 30, 2011

900

Settlement agreement: $1.7M

Boston Medical Center

March 4, 2014

15,000

Est. cost: $6M

- Third-party: Transcriptionist lacked technical safeguards on server
- Patient records accessible on Internet

Recent Breaches & Settlement Agreements

Anchorage Community Mental Health Services, Inc.

March 3, 2012

2,743 *patient records*

Settlement agreement: $150K

NewYork-Presbyterian / Columbia University Medical Center

September 24, 2010

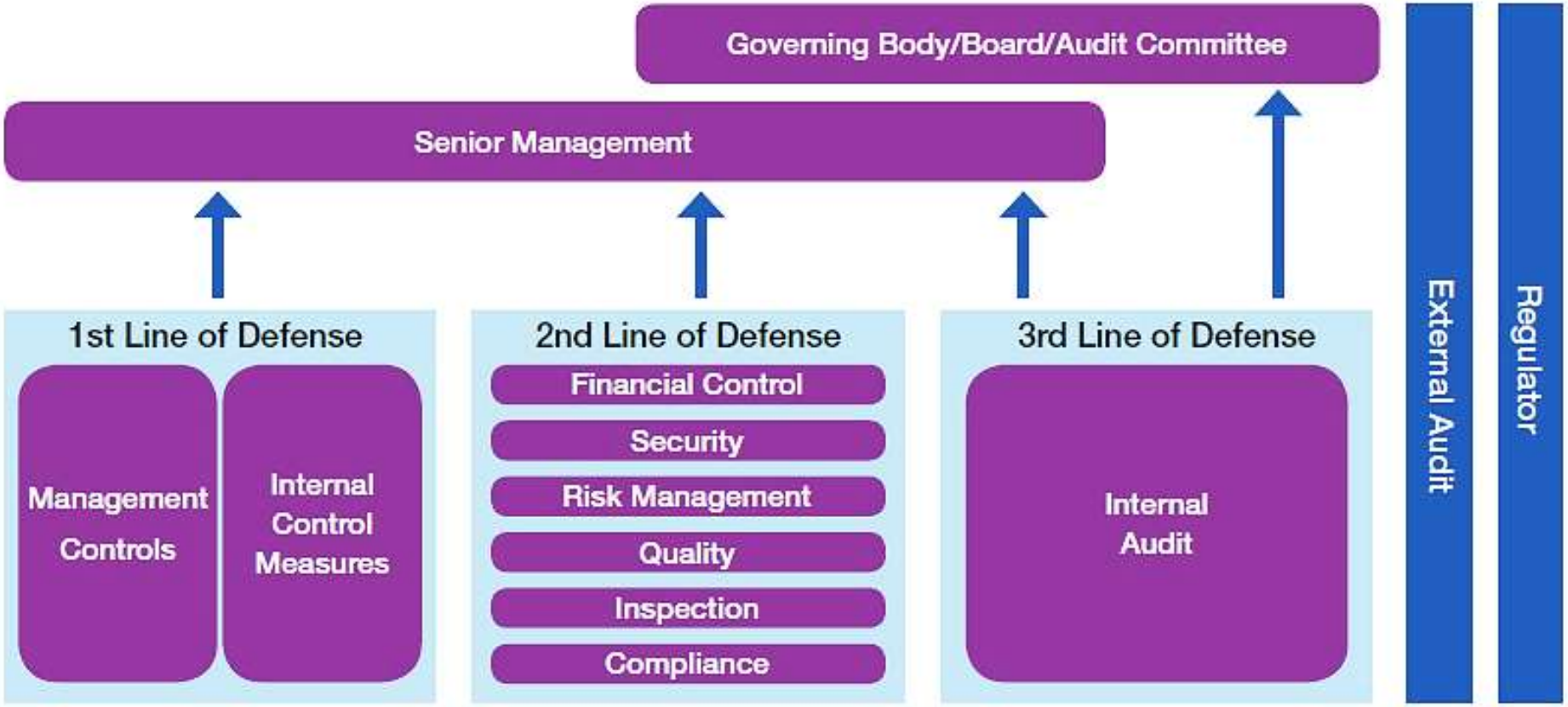
6,800

Settlement agreements: $3.5M NYP **$1.5M** CUMC

- ACMHS: Due to malware, fined for unpatched / unsupported systems
- NYP / CUMC: Server data accessible on the Internet due to lack of technical safeguards - Server installed and managed by a physician, not an IT professional

Cybersecurity – Not Just an IT Issue

- Board must assume role of fourth line of defense to protect against cyber risks within the whole organization



Board of Directors Responsibility

“A primary responsibility of every board of directors is to secure the future of the organization. The very survival of the organization depends on the ability of the board and management not only to cope with future events but to anticipate the impact those events will have on both the company and the industry as a whole.”

-Tom Horton, *Directors & Boards*

Why is Cybersecurity a Board Oversite Issue?

- Financial / reputational loss at a level relevant to the Board's fiduciary responsibility to sustain corporate mission
- Data breach laws make response costly / fines
- Class-action lawsuits are costly
- Consideration of cyber liability insurance
- Cybersecurity incidents disrupt operations
- Attackers include nation-states and organized crime targeting theft of trade secrets and economic sabotage
- Risks of disruption of industrial controls (smart buildings)
- Threat to medical devices

Five Guiding Principles for the Board

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

4. Directors should set the expectation that management will establish an enterprise-wide management framework with adequate staffing and budget.

5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Cyber-Risk Oversight Executive Summary, Director's Handbook Series 2014 Edition [National Association of Corporate Directors (NACD) in collaboration with AIG and Internet Security Alliance (ISA); Washington, DC; 2014]

Helping your Organization: Six Questions You Should Ask

1. Does the organization have a security framework and risk-based approach to security?
2. What are the top risks the organization has related to cybersecurity?
3. How are employees made aware of their role relating to cybersecurity?
4. Are external and internal threats considered when planning cybersecurity activities?
5. How is security governance managed within the organization?
6. In the event of a serious breach, has management developed a robust response protocol?

Six Questions You Should Ask

1. Does the organization have a security framework?

- HIPAA / HITECH, HITRUST (healthcare)
- PCI-DSS for credit card acceptance
- The National Institute of Standards and Technology (NIST) Cybersecurity Framework
  - President issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in Feb. 2013
- ISO 27001, NIST 800-53, COBIT

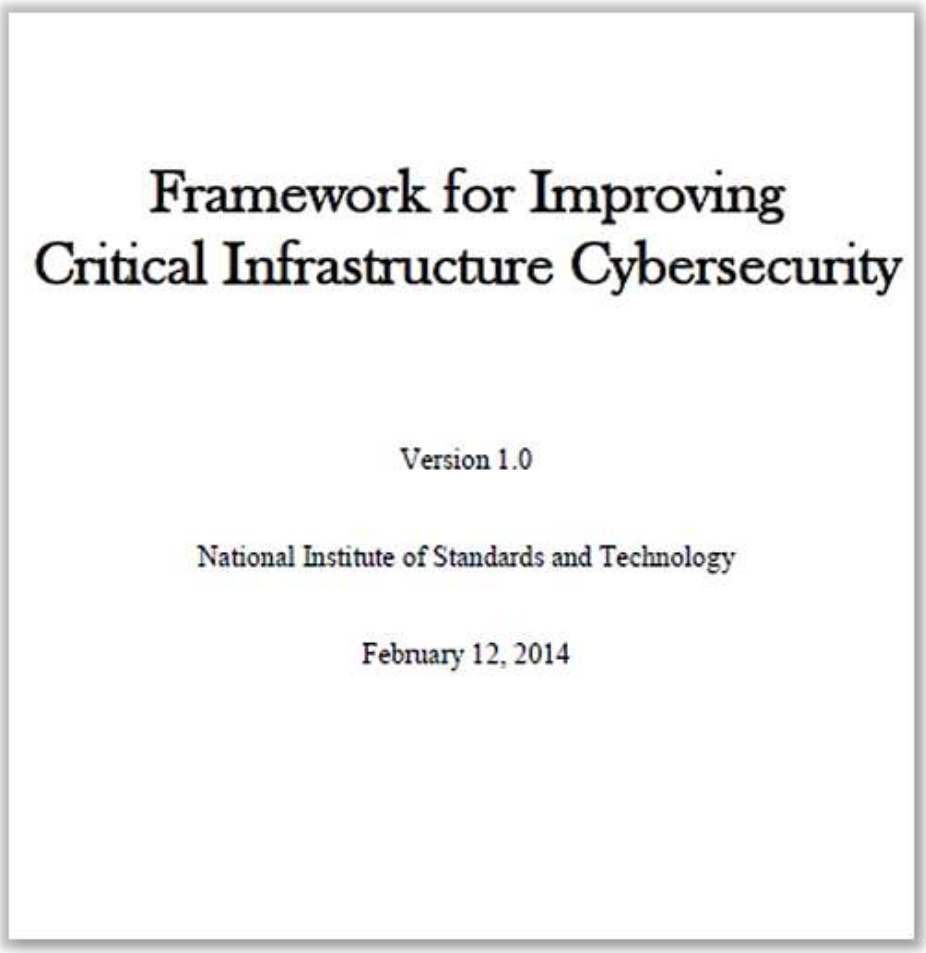
HIPAA Requires A Risk-Based Approach to Security

Protect against any **reasonably anticipated threats** or hazards 164.306(a)

Conduct a risk analysis: Apply a framework and **c**onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of [ePHI] held by the covered entity 164.308(a)(1)(ii)(A)

Risk management: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level 164.308(a)(1)(ii)(B)

National Institute of Standards & Technology (NIST) Cybersecurity Framework



Identify: Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy

Protect: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures

Detect: Anomalies and Events, Security Continuous Monitoring, Detection Processes

Respond: Response Planning, Communications, Analysis, Mitigation, Improvements

Recover: Recovery Planning, Improvements, Communications

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014

NIST Cybersecurity Framework

Benefits of using the **Cybersecurity Framework**:

- **Improve cybersecurity:** The NIST Framework core is up to date in terms of cyber threats / risks / effective controls – with an emphasis on Detect, Respond, Recover – not just Protect. It is much more up to date and comprehensive than the HIPAA rule.
- **Reduce legal exposure:** This process can demonstrate due care in case of a breach and federal / state investigation or even law suit. The NIST Framework is founded on a presidential order and represents best practices.
- **Improve collaboration and communication of security posture with executives and others**

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014

NIST Cybersecurity Framework

FRAMEWORK CORE

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8

Framework Core: a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.

Six Questions You Should Ask

2. What are the top risks the organization has related to cybersecurity?

Potential areas of risk (examples):

- Bring your own device (BYOD) and smart devices
- Cloud computing
- Outsourcing critical business controls to third parties (and lack of controls around third-party services)
- Disaster recovery and business continuity
- Hacking / malware / Advanced Persistent Threats
- Insider risks
- Medical device vulnerabilities

Healthcare Cybersecurity Risks: Third Party Risks

Third parties were the #2 cause of breaches in 2014[1]

Healthcare providers need to manage third party risks

- Evaluate whether third parties have access to PHI
- Evaluate the level of risk
- For high-risk third parties evaluate the security program
  - Before contracting
  - Ongoing
- Contract terms to manage third party risks

1 Identity Theft Resource Center: http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

Healthcare Cybersecurity Risks: Malware/Ransomware

Types of ransomware[1]

Locker:

- Restricts user access by either denying access to user interface or restricting availability of computing resources
- Typically spread through social engineering, phishing campaigns and watering-hole sites

Crypto:

- Encrypts and restricts access to data and file systems
- Typically spread through spam emails with Microsoft Word attachments, compromised websites and malvertising pages

1 *The ICIT Ransomware Report: 2016 Will be the Year Ransomware Holds America Hostage, © **2016,** by Scott, James and Spaniel, Drew, Institute for Critical Infrastructure Technology, 2016. Web. 26 Apr. 2016. http://icitech.org/wp-content/uploads/2016/ICIT-Brief-The-Ransomware-Report2.pdf*

Healthcare Cybersecurity Risks: Malware/Ransomware

Effective ways to keep your organization protected[1]:

- Employ a data backup and recovery plan for all critical information
- Use application whitelisting to prevent malicious software from running
- Keep your operating system and software up-to-date with the latest patches
- Contract terms to manage third party risks
- Restrict users' ability to install and run unwanted software applications
- Avoid enabling macros from email attachments
- Do not follow unsolicited Web links in emails

1 US-CERT: http://us-cert.gov/ncas/alert/TA16-91A

Healthcare Cybersecurity Risks: Insider Threats

"Insiders" refers to your workforce who are trusted with access to your systems

- They make mistakes
- They violate policies (snooping, shortcuts)
- A few have criminal intentions

Huge problem in healthcare!

Solutions

- Security awareness training
- Monitor / manage / discipline
- Access controls
- Data Leak Prevention
- User Activity Monitoring

Healthcare Cybersecurity Risks: Medical Device Vulnerabilities

Six Questions You Should Ask

3. How are employees made aware of their role relating to cybersecurity?

- Security awareness training program
- Review and annual test for employees
- Communication plan from CEO or other top executive

Six Questions You Should Ask

4. Are external and internal threats considered when planning cybersecurity activities?

Figure 2: The causes and consequences of cybercrime committed by insiders*

Most adverse consequences	Loss of confidential/proprietary data 11%	Reputational harm 11%	Critical system disruption 8%	Loss of current or future revenue 7%	Loss of customers 6%
Mechanisms used	Social engineering 21%	Laptops 13%	Remote access 17%	E-mail 17%	Copy data to mobile device 16%
Characteristics displayed	Violation of IT security policies 27%	Misuse of organization's resources 18%	Disruptive workplace behavior 10%	Formal reprimands/disciplinary action 8%	Poor performance reviews 7%
Reasons for committing cybercrime	Financial gain 16%	Curiosity 12%	Revenge 10%	Non-financial personal benefit 7%	Excitement 6%

** A current or former employee, service provider, authorized user of internal systems, or contractor*

US cybercrime: Rising risks, reduced readiness: Key findings from the 2014 US State of Cybercrime Survey, PwC

Six Questions You Should Ask

5. How is security governance managed within the organization?

- **1st Line of Defense**
  - IT operations function
  - Implements policies and standards
  - Day-to-day monitoring of networks and infrastructure
- **2nd Line of Defense**
  - Perform majority of governance functions related to cybersecurity
  - Headed by CISO, who defines policies, standards, and technical configurations
  - Ensure that IT performs monitoring, reporting, and tracking
- **3rd Line of Defense**
  - Internal audit ensures that 1st and 2nd lines of defense are functioning as designed

Six Questions You Should Ask

6. In the event of a serious breach, has management developed a robust response protocol?

- Incident response program / team / skills / tools
- Practice the program! Fail to plan, plan to fail!
- Crisis management program
- Crisis management team and their responsibilities

Questions?

Jim Hunter

Director, Monitoring and Security

CareTech Solutions