Security Is in the Spotlight

Use It to Your Advantage

©2014 Information Assurance Advisory, LLC

Presentation Agenda

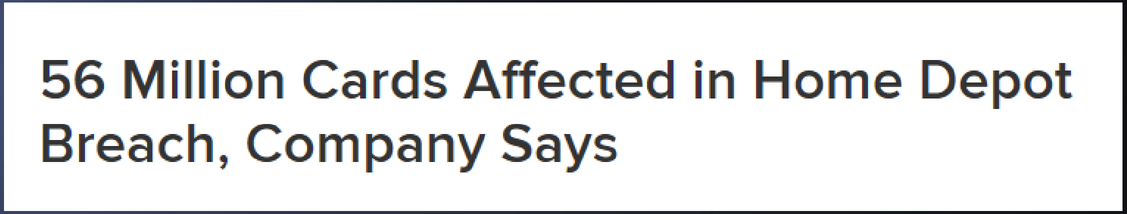
- Why demands and the strain on security staffs have increased.
- Beyond these demands, other items will require your attention.
- Capitalize on the increased focus to:
  - Improve operational risk management.
  - Invest in more integrated and robust analytical capabilities.
  - Implement a staffing strategy.

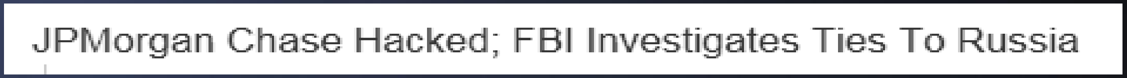
©2014 Information Assurance Advisory, LLC

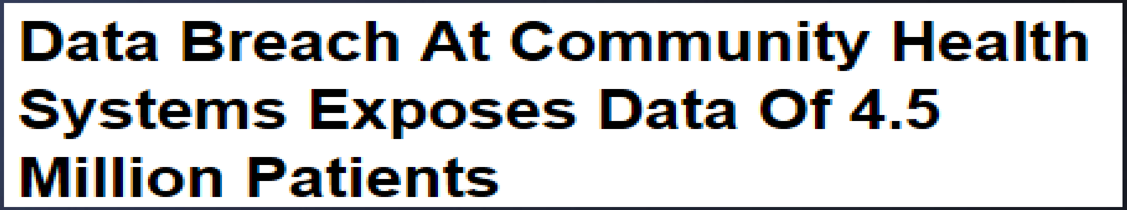
SYSTEM
INFILTRATED

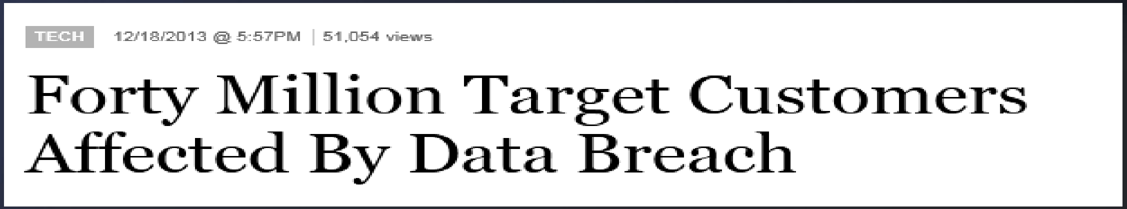
Headlines

Cybersecurity News
World · Business · Finance · Lifestyle · Travel · Sport · Weather

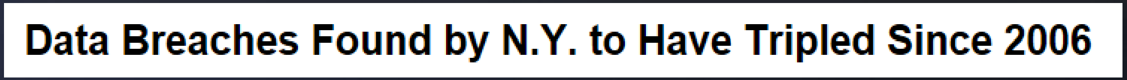

56 Million Cards Affected in Home Depot Breach, Company Says

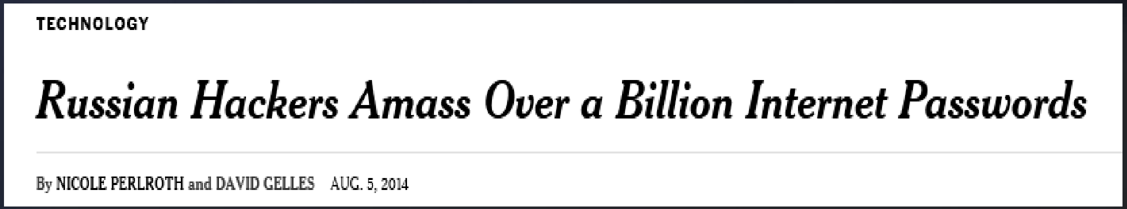

JPMorgan Chase Hacked; FBI Investigates Ties To Russia


Data Breach At Community Health Systems Exposes Data Of 4.5 Million Patients


TECH 12/18/2013 @ 5:57PM | 51,054 views

Forty Million Target Customers Affected By Data Breach


Data Breaches Found by N.Y. to Have Tripled Since 2006

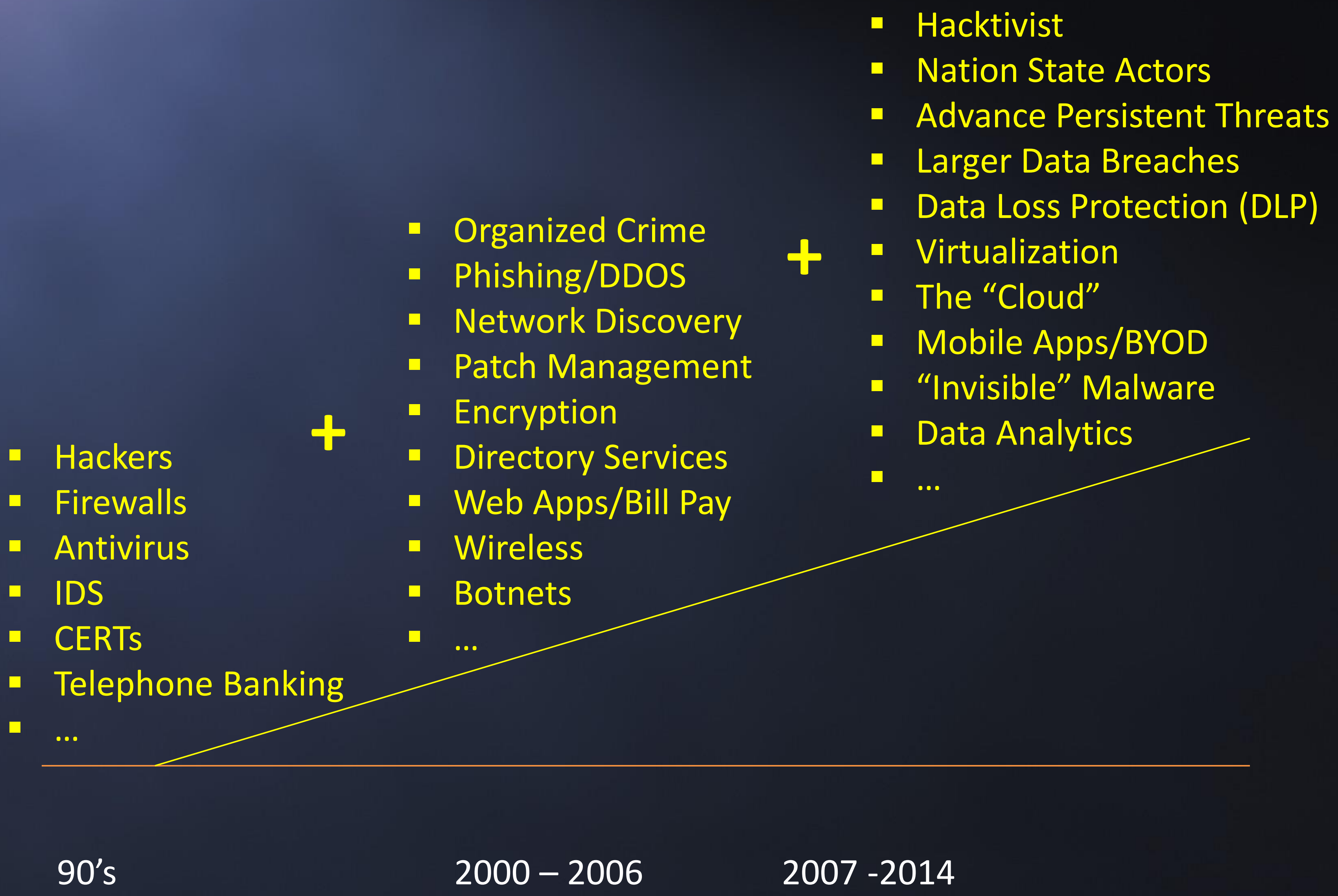

TECHNOLOGY

Russian Hackers Amass Over a Billion Internet Passwords

By NICOLE PERLROTH and DAVID GELLES AUG. 5, 2014

©2014 Information Assurance Advisory, LLC

Demands on Security Staffs Have Been Expanding



- Hackers
- Firewalls
- Antivirus
- IDS
- CERTs
- Telephone Banking
- …

+

- Organized Crime
- Phishing/DDOS
- Network Discovery
- Patch Management
- Encryption
- Directory Services
- Web Apps/Bill Pay
- Wireless
- Botnets
- …

+

- Hacktivist
- Nation State Actors
- Advance Persistent Threats
- Larger Data Breaches
- Data Loss Protection (DLP)
- Virtualization
- The “Cloud”
- Mobile Apps/BYOD
- “Invisible” Malware
- Data Analytics
- …

90’s

2000 – 2006

2007 -2014

©2014 Information Assurance Advisory, LLC

“Invisible” Attack

Heartbleed*

Vulnerability of Open SSL cryptographic software library.

Caution !

- This was open source security software.
- Known type of software weakness exploited.
  - CWE-20: Improper Input Validation.

Sept. 24, 2014: Bash/Shellshock Vulnerability Disclosed

This flaw involves extra code added to the end of certain Unix and Linux functions that allows remote attackers to execute arbitrary code.

©2014 Information Assurance Advisory, LLC

* IBM Analysis - http://securityintelligence.com/heartbleed

“Invisible” Malware

- Earlier malware was a file detected by antivirus (AV) programs.
- Newer forms of malware use techniques to remain invisible and persistent.
  - An Example: “Poweliks”*
    - Resides in the Windows registry only
    - Malicious activity performed in memory (no file created)
    - Reactivated on system reboot (persistent)

Will get worst

©2014 Information Assurance Advisory, LLC

* *Based on G Data Security Labs Analysis <https://blog.gdatasoftware.com>*

Mobile Device Angst

BYOD (Bring Your Own Device)

Who's in the Middle ?

Business Groups -> **The Security Organization** <- Employees

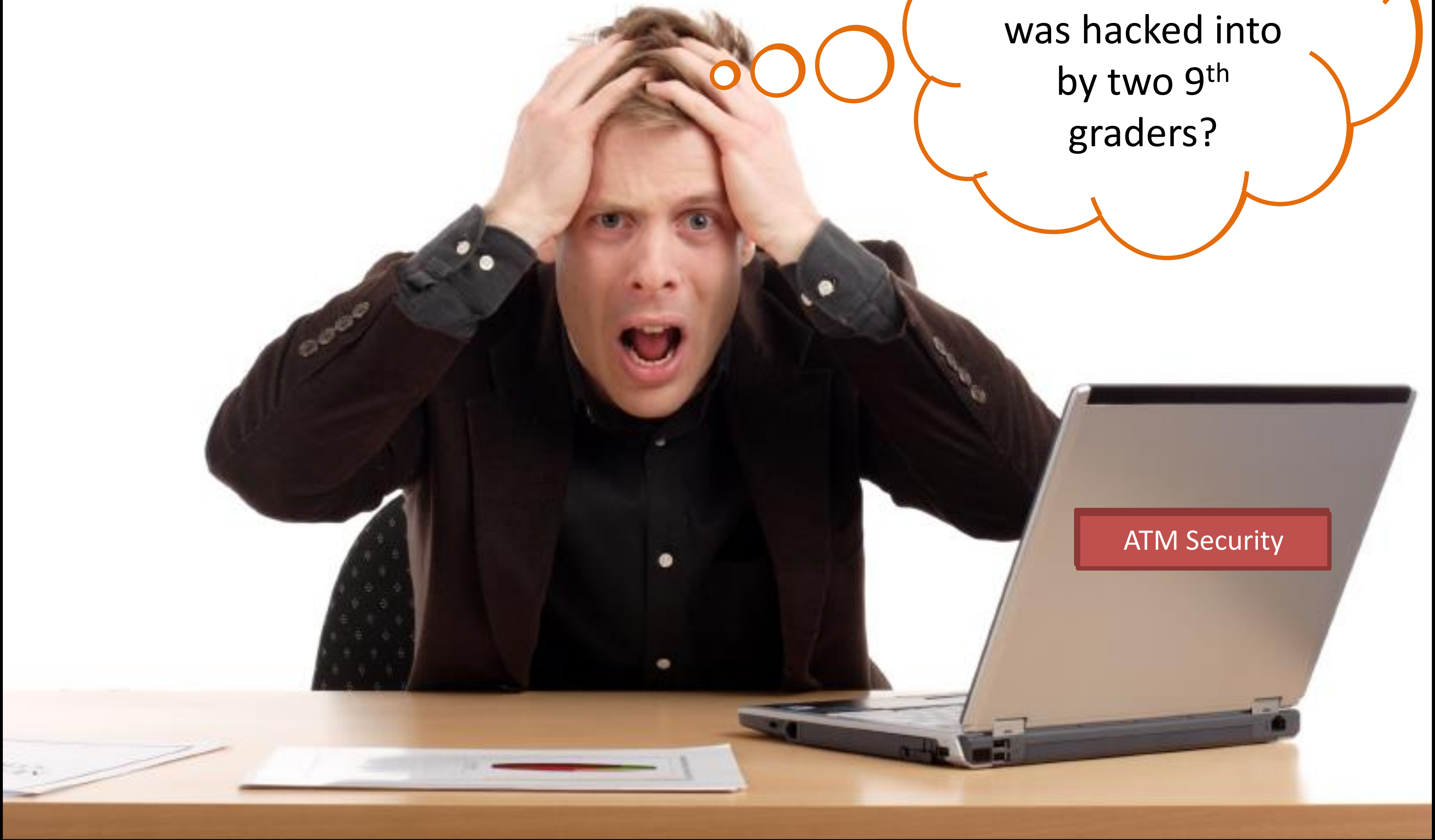
Exploitive Apps, loss devices, data leakage, loss of login credentials, etc.

Court cases will have an impact

©2014 Information Assurance Advisory, LLC

What's your worst nightmare?

How do I tell my boss our ATM was hacked into by two 9th graders?



ATM Security

©2014 Information Assurance Advisory, LLC

… and the Spotlight Is Going to Get Brighter.

Why ?

- ✓ *Laws and Regulations*
- ✓ *Increasing Privacy Concerns*
- ✓ *More Medical Records Online*
- ✓ *The Internet of Things (IoT)*
- ✓ *Nation-state Cyber-warfare*

©2014 Information Assurance Advisory, LLC

Laws and Regulations Expanding

Additional work with your …

Legal Counsel
Auditors
Contracts Organization

DUTY OF CARE
RISK OF MATERIAL MISTATEMENTS
REQUIREMENTS and LIABILITIES

Drivers

- Health Care
  - Health Insurance Portability and Accountability Act
- Financial Industry
  - Gramm-Leach-Bliley Act
- Public Companies:
  - Sarbanes-Oxley
  - SEC Cyber Disclosure Requirements
- All Organizations:
  - Data Breach Disclosures
  - Federal Trade Commission (FTC) Actions

©2014 Information Assurance Advisory, LLC

FTC Data Security Actions

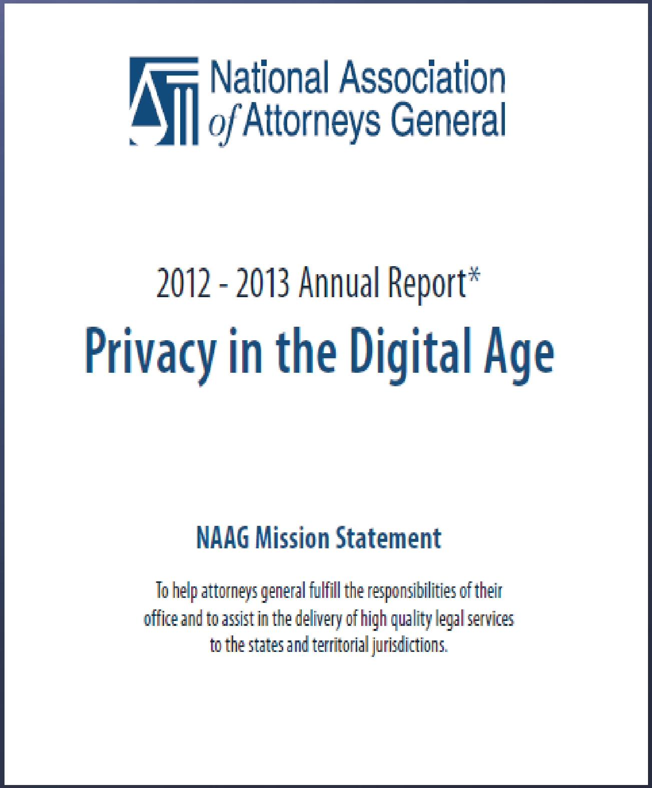
- "The FTC has settled 50 cases against companies that we alleged put consumer data at risk." FTC Chairman*
- Allege "Failure to maintain reasonable and appropriate data security."
- Examples:
  - Wyndham Worldwide Corporation — franchises hotels
    - Three breaches of its reservation system: 2008 – 2010
    - Ongoing case — Wyndham challenged FTC jurisdiction (Court Denied)
  - HTC America, Inc. — mobile phone maker
    - Alleged HTC undermined Android security model and increased other security risks to users of its phones.
    - Also alleged it failed to listen to vulnerability reports.
    - Settled without admitting liability.

FTC is asking congress for broader authority to go after nonprofits, such as universities and health systems.

** FTC Chairman testimony to Congress March 26, 2014*

©2014 Information Assurance Advisory, LLC

Increasing Privacy Concerns



National Association of Attorneys General

2012 - 2013 Annual Report*

Privacy in the Digital Age

NAAG Mission Statement

To help attorneys general fulfill the responsibilities of their office and to assist in the delivery of high quality legal services to the states and territorial jurisdictions.

- State Attorneys General offices staffing up their cybersecurity and privacy expertise.
- Enhancing communications and coordination among state offices.
- States establishing enforcement organizations.
- Data breaches create more consumer complaints.
- Collaborating with the FTC.

Data usage and security protection practices will get increased focus

©2014 Information Assurance Advisory, LLC

More Medical Records Online

- The Health Insurance Portability and Accountability Act of 1996
- Health Information Technology for Clinical and Economic Health (HITECH) Act of 2009
- The *Omnibus Rule* was issued by Health and Human Services (HHS) Jan. 25, 2013

©2014 Information Assurance Advisory, LLC

More Medical Records Online *(cont'd)*

- Complicated rules apply to: -

COVERED ENTITY ← Health care provider, clearinghouse or provider who transmits any covered information

BUSINESS ASSOCIATE ← Partner providing services involving individually identifiable health information

A portion of your business may be providing partner services

©2014 Information Assurance Advisory, LLC

The Internet of Things (IoT)

Embedded systems pose unique security problems.

Implementation in connect systems must be part of risk assessments.

Can be overlooked or not understood.

There is a lack of industry standards.

Fertile area for researchers and hackers.

Expands the attack surface

©2014 Information Assurance Advisory, LLC

More Nation-State Cyber-Warfare Implications

- Organizations can be targets or experience collateral damage from nation-state cyber-warfare efforts.
- Well-funded terrorists increase the concern.
- Cyber weapons pollinating commercial malware:
  - Knowledge transfer (e.g., APT Malware)
  - DDOS capability growth

Is your organization a member of a critical infrastructure?

©2014 Information Assurance Advisory, LLC

CAPITALIZING ON THE INCREASED ATTENTION

©2014 Information Assurance Advisory, LLC

Improve Operational Risk Management

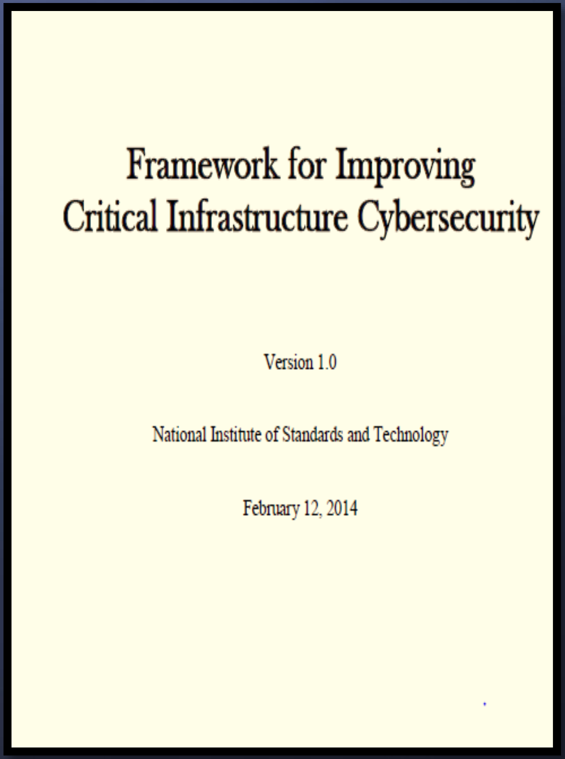
Who assists the CEO in assessing and managing the operational risk in your organization?

- Board of Directors
- Line-of-Business Executives
- Chief Information Officer
- Chief Technology Officer
- Chief Information Security Officer
- Head of Physical Security
- General Counsel
- Chief Auditor

External requirements offer a new opportunity to increase business–based risk management In your organization.

©2014 Information Assurance Advisory, LLC

Adopt U.S. Cybersecurity Framework



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

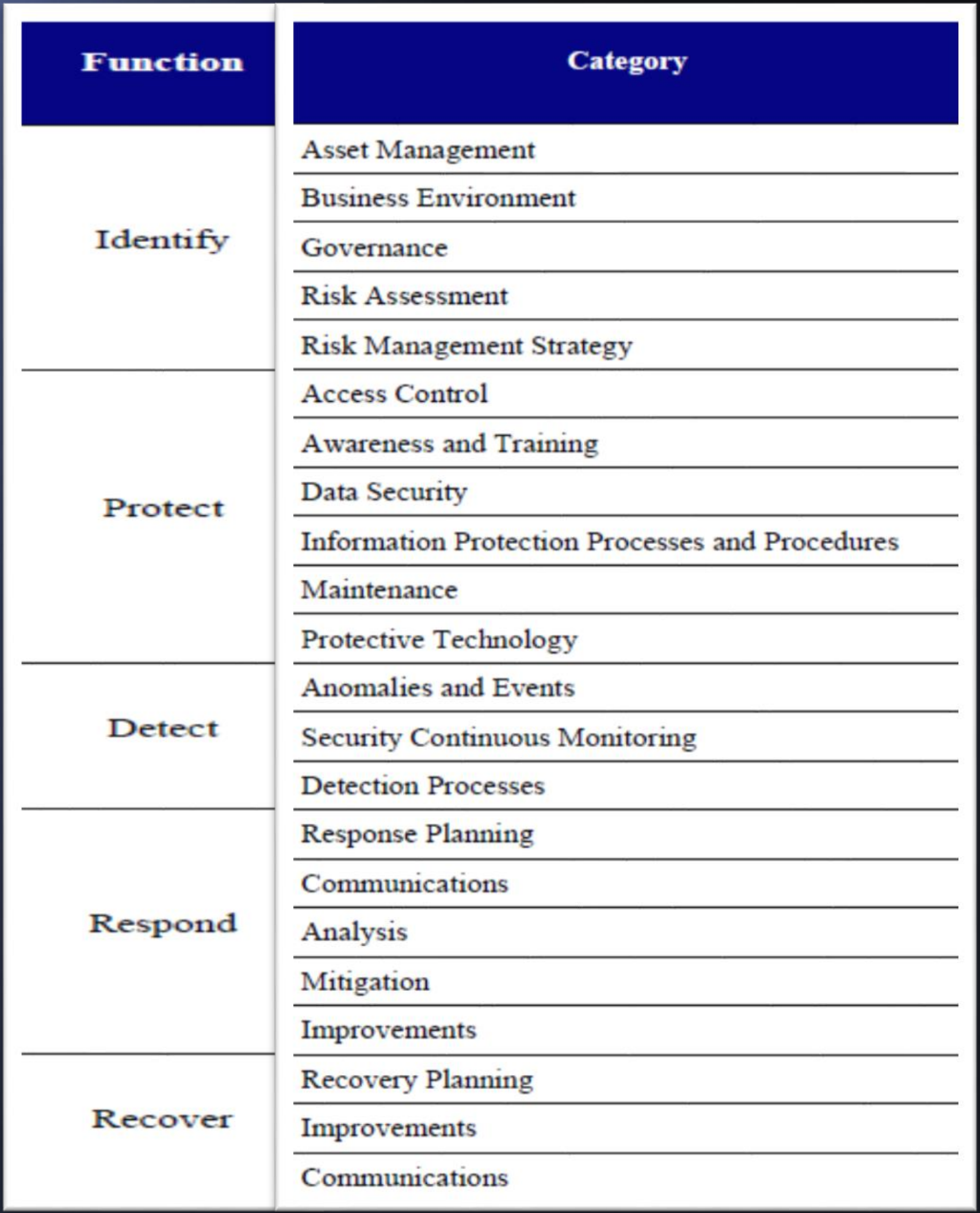
- Published February 2014
- Created with much industry input
- Business risk-assessment based
- Lets you examine if you're covering the basics.
- Numerous references

Partner with Legal to force adoption. Why?

Because it will be a basis for fulfilling "Duty of Care"

©2014 Information Assurance Advisory, LLC

Key Elements of the Framework



Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

©2014 Information Assurance Advisory, LLC

Invest in More Robust Analytical Capability

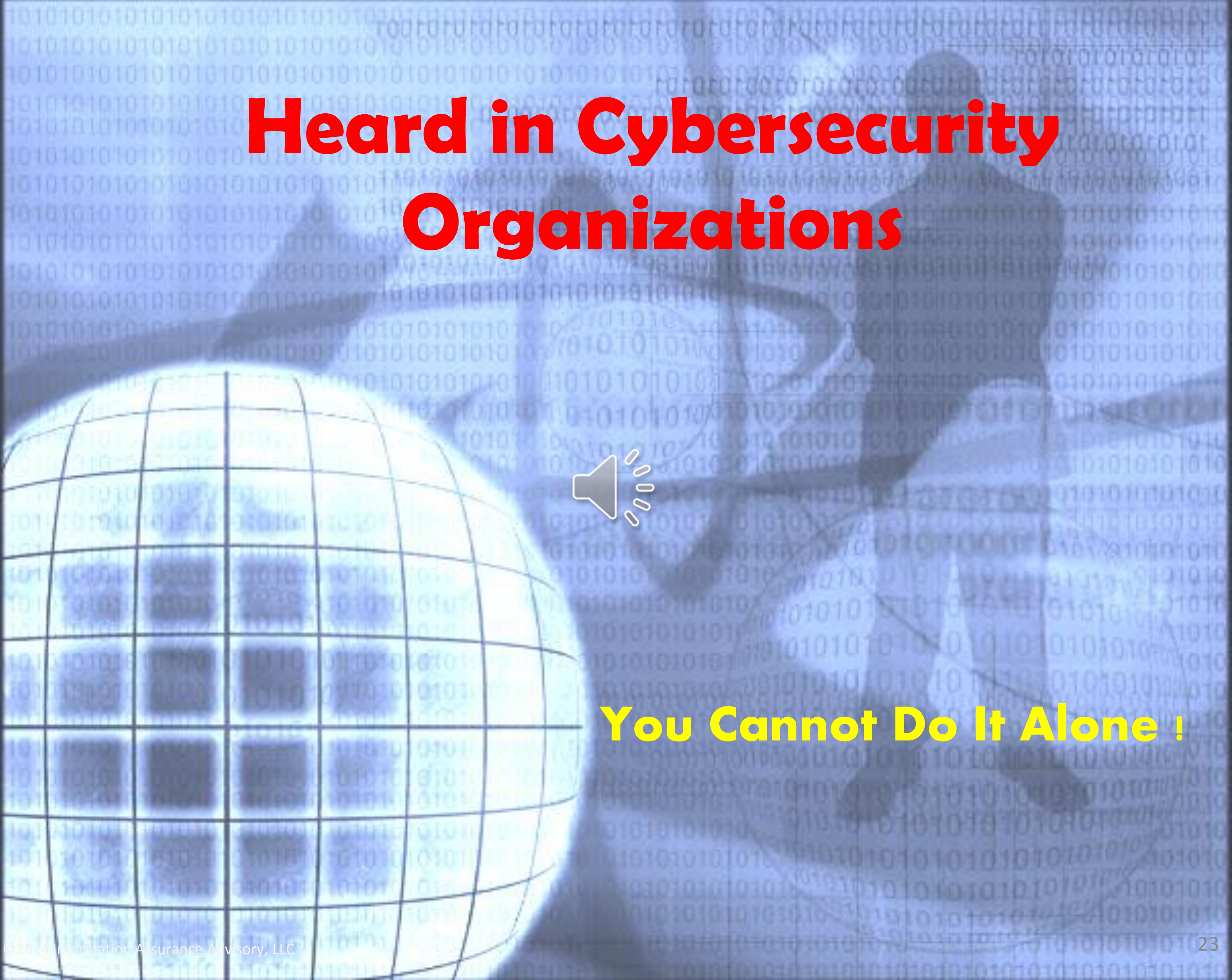
Organizations swamped with disparate data repositories and a need for timely analytics

Financial sector spearheading threat intelligence and other automation

Apply classic intelligence functions to the challenge.

Collection – Analysis - Reporting

©2014 Information Assurance Advisory, LLC



Heard in Cybersecurity Organizations

You Cannot Do It Alone !

©2014 Information Assurance Advisory, LLC

Implement a Staffing Strategy

- Consider the expanding demands discussed
- Establish your staffing requirements
- Develop a staffing strategy
    1. Increase resources to hire scarce skills or train associates who can help.
    2. Pursue resources for additional managed services.
    3. A combination of both.

Doing nothing is not an option

©2014 Information Assurance Advisory, LLC

Capitalize on the Increase Attention

Summary

- Improve operational risk management.
  - Adopt U.S. Cybersecurity Framework
- Invest in more integrated and robust analytical capabilities.
- Implement a staffing strategy.

©2014 Information Assurance Advisory, LLC

Discussion

Email: roger.callahan@iaadvisory.com

Phone: 704-236-2385

©2014 Information Assurance Advisory, LLC