FrankenLaws:

The Sad State of the Information Security Regulatory Landscape

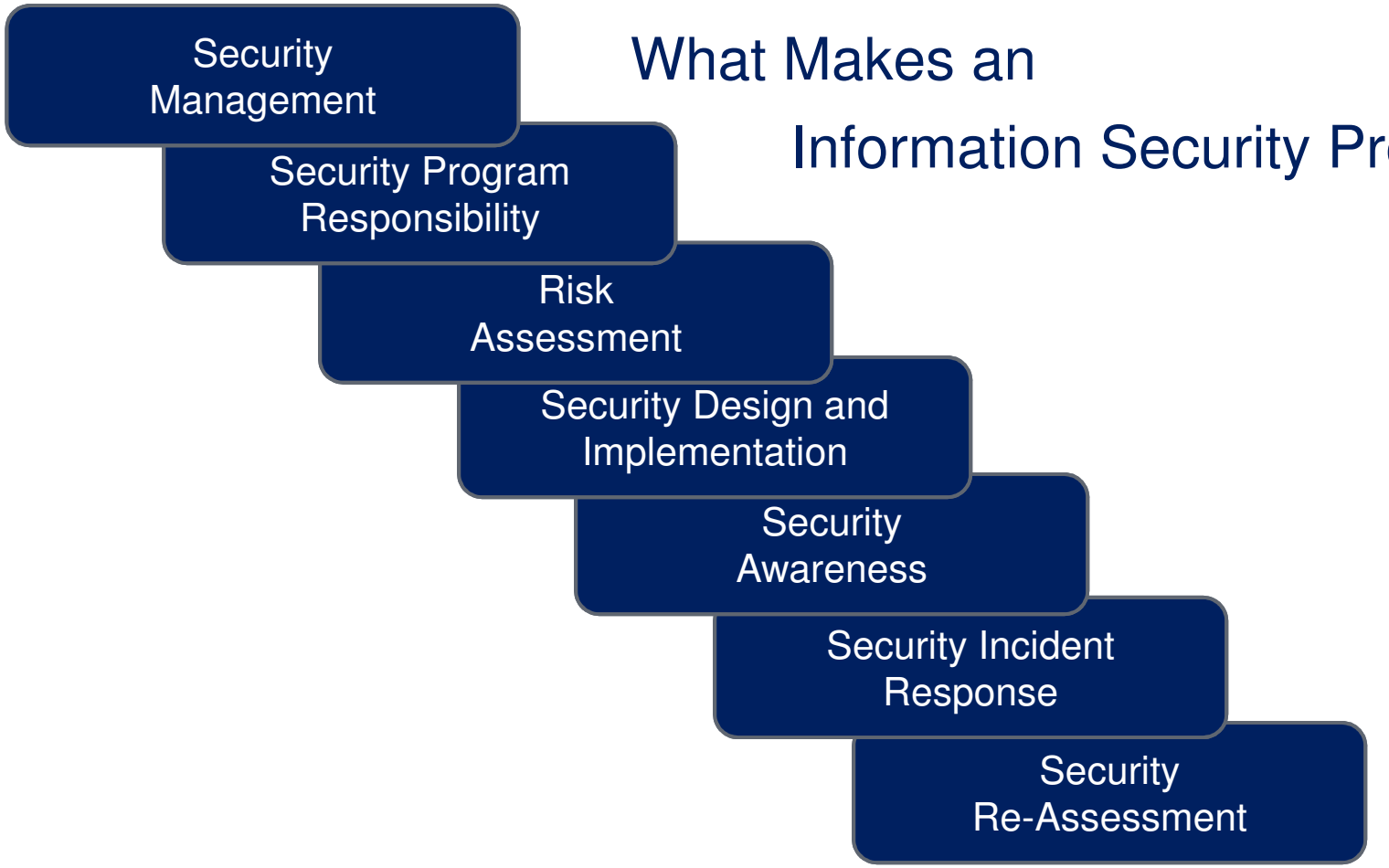
UNCC 12th Annual Cyber Security Symposium
Tuesday, October 11, 2011
Charlotte, North Carolina

John Linkous | Vice President, Chief Security & Compliance Officer | eIQnetworks, Inc.

The Goal: Reasonable Security

- **Make systems – and the data stored on them – more secure**
  - Cardholder Data
  - ePHI
  - Intellectual Property
  - Classified / Intelligence Data
  - Business- and Mission-Critical Systems
  - Wired and Wireless Networks
  - Applications and Databases
  - Network Infrastructure Connectivity
- **Reduce the likelihood of threats to an acceptable level**
  - Data Breaches (cardholder data, ePHI, intellectual property)
  - Malware, Phishing and Externally-Launched Attacks
  - Insider Threats
  - Advanced Persistent Threats
  - Threats from Emerging Technologies (Cloud, Mobile, etc.)
- **Verify that bad stuff isn't happening**

What Makes an Information Security Program?



Source: OECD Guidelines for the Security of Information Systems and Networks

Today's Security Framework: Federal Laws

- Healthcare Data-Specific
  - **Health Insurance Portability and Accountability Act (HIPAA)**
  - **HITECH Act**
- Financial Reporting Data-Specific
  - **Sarbanes-Oxley (SOX)**
- Consumer Data-Specific
  - **Gramm-Leach-Bliley (GLBA)**
- Federal Government-Specific
  - **Federal Information Systems Management Act (FISMA)**

Today's Security Framework: Regulatory Agencies

- Financial Services Industry
  - **SEC**
  - **FDIC**
  - **NCUA**
  - **FTC**
- Energy Industry
  - **FERC**
- Healthcare Industry
  - **Department of Health and Human Services (DHHS)**
  - **Centers for Medicare & Medicaid (CMS)**
  - **Joint Health (JHACO)**
  - **Office of Civil Rights (OCR)**
  - **CMS/JHACO (Healthcare)**

Today's Security Framework: International Law and Best Practices

- Best Practice Frameworks *(voluntary)*
  - **ISO 27001/27002**
  - **COBIT**
  - **NIST 800-53**

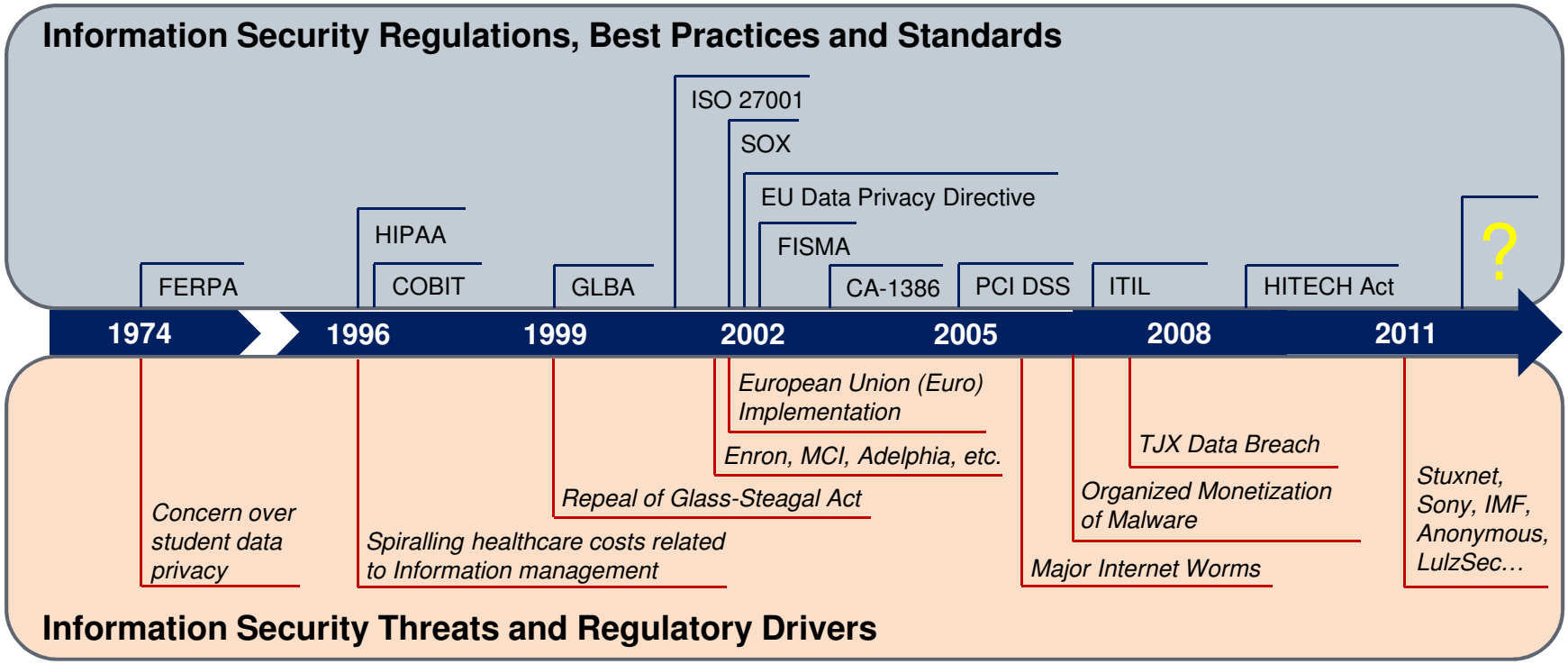
- Business Agreements *(mandatory)*
  - **PCI Data Security Standard (DSS)**

- International & Jurisdictional Privacy and Security Laws
  - **EU Data Protection Directive (EU Nations)**
  - **US Dept. of Commerce "Safe Harbor" (dealing with EU nations)**
  - **PIPEDA (Canada)**
  - **J-SOX (Japan)**
  - **ITAR (United Nations)**

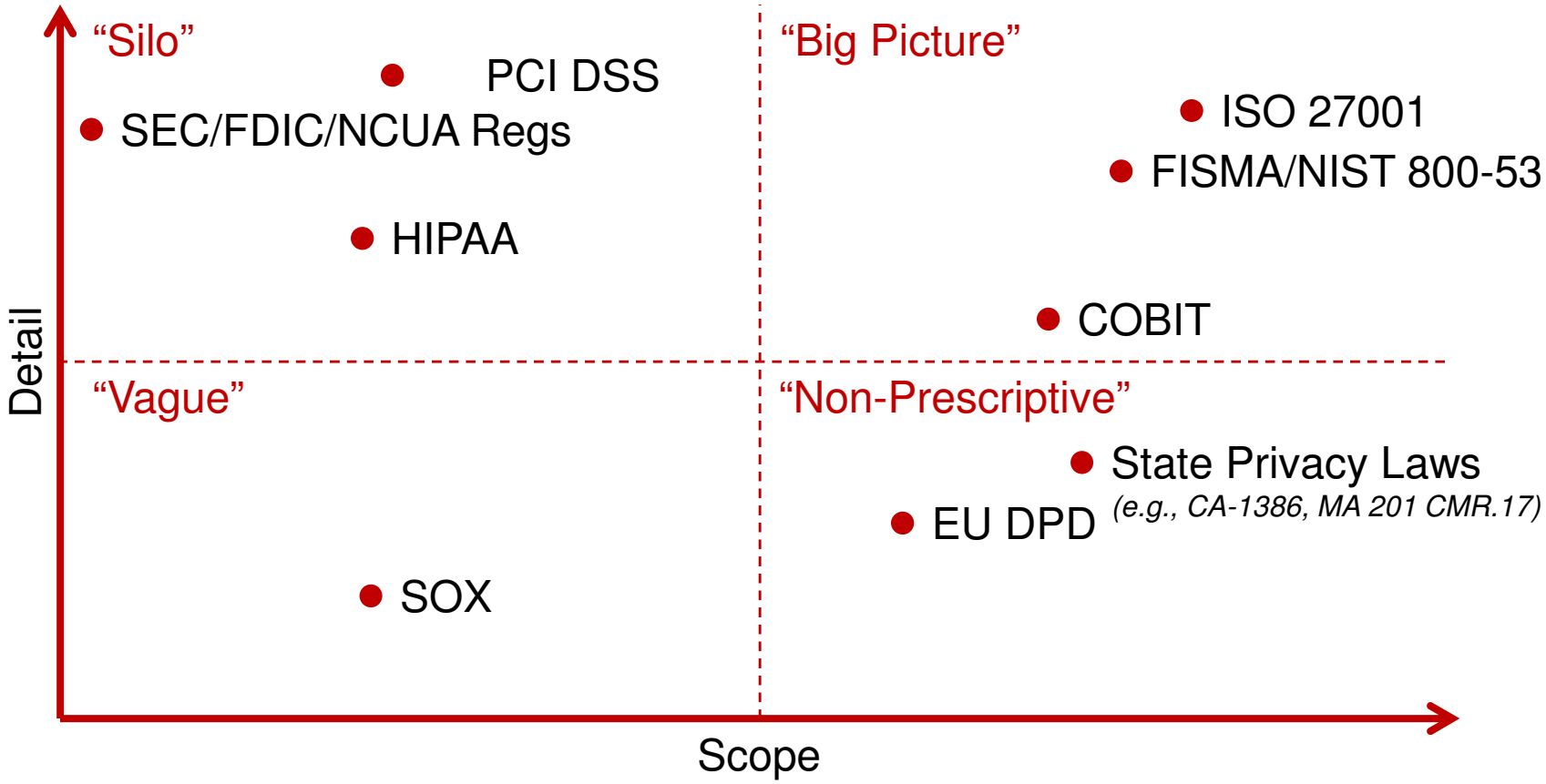
Pending Legislation

- **Cybersecurity Act of 2010**
  - Sponsors: Rockefeller (D-WV); Bayh (D-IN); Mikulski (D-MD); Nelson (D-FL); Snowe (R-ME)
  - Defines “critical infrastructure” and “infrastructure in the national interest”
- **International Cybercrime Reporting and Cooperation Act**
  - Sponsors: Clarke (D-NY), (6) Democrats, (1) Republican
  - Provides the President with enhanced legal, judicial and enforcement remedies for international cybercrime
- **Protecting Cyberspace as a National Asset Act of 2010**
  - Sponsors: Lieberman (I-CT); Collins (R-ME); Carper (D-DE)
  - Contains the “Internet kill switch” language
- **President’s Proposed Cybersecurity Legislation**
  - Sent by Executive Office of the President (EOP) to Congress on 5/12/10
  - Recommended developing legislation to force security in private industry critical infrastructure

A Brief History Lesson: How Did We Get Here?!?



FrankenLaw: Inconsistent Scope & Detail



FrankenLaw: "Vague" Security Mandates

- Pros
  - Focused on a specific business problem that needs to be fixed
  - Sometimes (but not always) provide additional guidance (e.g., point to best practice standards)

- Cons
  - Outrageous implementation costs due to vague prescriptions
  - Wildly varied audit and assessment standards
  - Hard to "pin down" the right implementation solution
  - Subject to lots of vendor FUD

FrankenLaw: "Silo" Security Mandates

- Pros
  - Define pretty good, well-rounded controls
  - Establish processes that can be extended to other systems
  - Often a good "starting point" for a security program

- Cons
  - Focused only on a limited set of systems and/or data
  - Zero interest in systems outside their scope
  - Controls for "Y" assets may not be appropriate for "Z" assets

FrankenLaw: "Non-Prescriptive" Security Mandates

- Pros
  - Designed to address a broader set of data and/or systems
  - In spirit, form the basis of a fairly complete security and/or privacy program

- Cons
  - Incomplete set of defined processes, controls and specifications
  - Tells you *what* needs to be done; doesn't really tell you *how*
  - *"The Road to Hell is paved with good intentions"*
    – John Ray, 1670

FrankenLaw:
"Big Picture" Security Mandates

- Pros
  - Complete security programs *(for the most part…)*
  - Flexible: controls and processes can be modified based on individual organizational risk

- Cons
  - Can be unwieldy; generally require tools/technologies to map enterprise data into the controls
    - IT GRC platforms
    - Situational Awareness platforms
  - Expensive to implement, especially if you use certified auditors
  - Content itself sometimes requires licensing (e.g., ISO 27001)
  - Most importantly… these are rarely *mandated*!

FrankenLaw: Overlaps & Gaps

	SOX	PCI DSS	Mass. Privacy Law	ISO 27001
Scope	Financial Reporting Systems	Cardholder Data	MA Resident Personal Data	Everything
Risk Management	N/A	Yes *(any model)*	Yes *(proprietary)*	Yes *(NIST 800-30)*
Third-Party Service Provider Management	N/A	Yes	Yes	Yes
Password Minimum Length	N/A	7 characters	N/A	"quality passwords"
Anti-Malware Components	N/A	"latest"	"reasonably up-to-date"	"as appropriate"

FrankenLaw:
Failure to Address Modern Threats – Social Media

- Over-sharing company information
- Mixing personal and professional information
- Engaging in SM rage
- Believing he/she who dies with the most connections wins
- Password sloth
- Trigger finger, AKA Wanton clicking
- Endangering yourself or others

Source: CSO Magazine, June 30, 2009

FrankenLaw:
Failure to Address Modern Threats – Mobile

- Trojanized QR codes
- Social Media Malware Infiltration / Sandboxing
- Trojanized “App Store” Apps
- Application Privilege Over-Use

FrankenLaw:
Failure to Address Modern Threats – Cloud

- Privileged user access
- Regulatory compliance
- Data location
- Data segregation
- Recovery
- Investigative support
- Long-term viability

Source: Gartner, "Assessing the Risks of Cloud Computing", June, 2008

Closing the Gap: What New Regulations Need to Do

- **Outcomes-Driven Legislation**
  - Focus on goals (e.g., “establish measurable information risk”, “reduce vulnerabilities”, “protect high-value data”)
  - Don’t force specific policies or controls; there are too many variances across industries and technologies
  - Utilize existing industry-specific regulatory bodies (e.g., FERC, SEC, CMS/JHACO) to identify the industry-specific controls

- **Area of Concern: Advanced Technologies = Advanced Threats**
  - Devices, data and applications are located everywhere around the world
  - Broad-based mandates (e.g., “maintain centralized control of all critical data”) may not be feasible without tremendous re-engineering and cost (e.g., separation of systems under SOX, PCI DSS)

Closing the Gap: What New Regulations Need to Do

- **Improve Public-Private Partnership**
  - Focus on one group – e.g., DHS/US-CERT, USCYBERCOM, DISA or NIST – and have that group be the primary interface between public policy and private industry
  - Improved awareness of current methods of public-private partnership; many private organizations don't know what services and tools are available for free from agencies

- **Minimize the Cost Burden**
  - Provide tax credits for successful implementation of cybersecurity policy will go a long way toward voluntary buy-in of mandated security and privacy legislation

OK, So What Do I Need to Do Today?

- **Build a Compliance Program**
  - Don't build regulation-specific programs "HIPAA Program", "SOX Program"
  - Your organization already has to comply with multiple regulations, best practices and standards… whether they realize it or not
  - Take a "greatest common denominator" approach to controls

- **Got Visibility?**
  - You need visibility into a broad range of security-related data
  - Individual point tools – SIEM, DLP, DAM, NAC, IDS/IPS – are not going to cut it on their own
  - Consider an IT GRC or Situational Awareness solution to give you the holistic visibility you need

OK, So What Do I Need to Do Today?

- **Keep on Top of Regulations, Best Practices and Standards**
  - It's a rapidly-changing landscape out there
  - Work with your auditors to implement their recommendations to close compliance gaps

- **Consider the Compliance Impact of All New Technologies**
  - Make sure that compliance impacts of all new technologies are reviewed before these technologies are bought and implemented

Predictions:
Where Will We Be in 10 Years?

- **Prediction #1: A National Privacy Law**
  - Unlike Europe and many individual countries, the US does not yet have a unified privacy law
  - The federal government will establish a privacy law that supersedes individual state laws, and establishes a framework for the safe handing of personal information on US citizens

- **Prediction #2: No More Vague "SOX"-like Laws**
  - Experience has shown that the cost of "Vague" laws is too extreme, and the effectiveness is too hard to measure
  - Any laws between now and then will more detailed and prescriptive

Predictions:
Where Will We Be in 10 Years?

- **Prediction #3: Federal "Cybersecurity" Legislation Extends to Private Industry**
  - Already, the federal government is implementing security standards for "critical infrastructure" systems (energy production/distribution, food/water supply management, transportation)
  - Expect additional laws – perhaps a single law that gets re-evaluated every year – to address minimum security controls that get applied to systems across many industries (financial, energy, public services, etc.)

- **Prediction #4: Existing Laws Will be "Updated" with Guidance for New and Emerging Threats**
  - Laws and best practices lack controls and processes to address emerging threat vectors such as mobile devices and cloud computing
  - Expect organizations that issue or audit these existing laws and standards (e.g., ISACA, ISO, PCI, CMS, etc.) to issue new "guidance" documentation to address how their controls should be applied to emerging technologies

Predictions:
Where Will We Be in 10 Years?

- **Prediction #5: Nation-State Actors Come Front-and-Center**
  - Because of the increasing concern of nation-state actors as malicious attackers, regulations (most likely at the federal or possibly international level) will establish the need for organizations to evaluate connectivity based on “reputation”, and potentially disconnect access based on geographic location

- **Prediction #6: Increased Focus on Continuous Monitoring**
  - Simply implementing controls isn’t enough
  - Organizations – and auditors – will be focused on ensuring that organizations that implement controls need to continuously monitor them for effectiveness
  - You’ll see a much stronger focus on “situational awareness”

Predictions:
Where Will We Be in 10 Years?

- **Prediction #8: Despite All These Advances in Security Legislation, Bad Things Will Still Happen**
  - There is no such thing as a 100% secure system
  - Bad people – especially in the cyber world – are incredibly smart
  - New attack vectors will be discovered, data will be breached, and critical systems will be affected
  - Regardless of mandates, some organizations will simply respond to them with EPIC FAIL implementations
  - ***But hopefully…*** the results of these incidents will be studied, and applied to future guidance on existing regulations

Thank You!

- **Questions?**
- **Comments?**

- **John Linkous**
  Vice President, Chief Security and Compliance Officer
  eIQnetworks, Inc.
  jlinkous@eiqnetworks.com