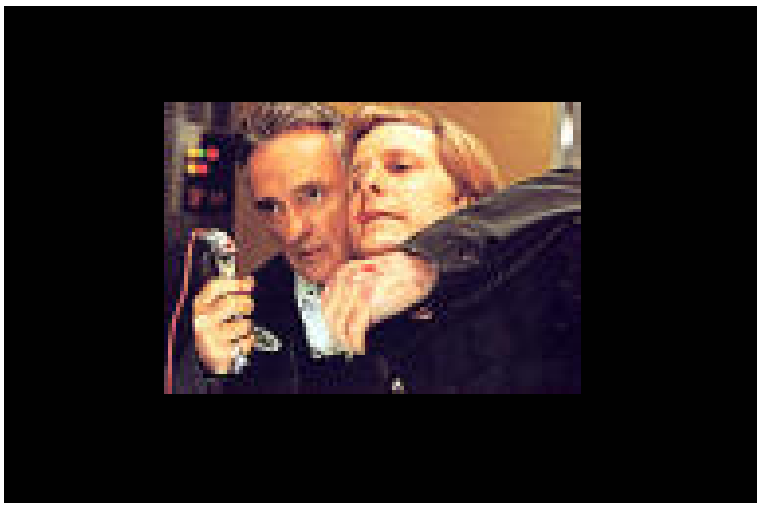
High Risk Information: Safe Handling for System Administrators

Lance Hayden
Cisco Advanced Services for Network Security
Austin, Texas
lhayden@cisco.com

The HRI Dilemma

“Pop quiz, hot shot – you have information located somewhere in your systems that threatens your users, your customers, your board, and your network...”



“What do you do?”

“What *do* you do…?

Let’s Walk Through It…

- Who’s Lance?
- Origins of the HRI concept and this talk
- What makes information into HRI?
- Some current drivers
- An HRI Protection Framework
- The future as I see it
- Conclusions and Q&A

My Background

CISCO SYSTEMS

HRI Concept

- Idea developed in my academic research
- Defined parallels in corporate & public worlds
- Some information carries an associated risk
  - Social risk
  - Business risk
  - Legal risk
  - Technical risk
- Both and old and a new idea, but new laws and social issues are bringing it to the forefront
- …and it can affect you directly.

HRI Typology (Basic)

- **Social**: ***information that is perceived as detrimental, harmful, unacceptable, or illegitimate under the existing social, cultural, or political structures and norms in place within the environment in which the information seeker is operating***
- **Influential**: ***information that is capable of exerting influence over the behavior or decisions of others within the larger societal or political framework***

HRI Typology (Basic)

- **Legal**: ***information that, by mandate or decree of an authority structure, has been proscribed***
- **Technical**: ***information that informs the user of technical attributes and more specifically technical vulnerabilities in existing systems***
- **Misinformation**: ***information that is not factual, by common consensus of fact, or is factual but in a way that distorts the larger conclusions to be drawn from those facts***

What Makes HRI?

- **Any information can be HRI when properly contextualized:**
  - **Credit card numbers**
  - **Listserv membership info**
  - **Logs and caches (IM, Web, etc.)**
  - **System configurations**
  - **Digital representations (images, movies, sounds)**
- **The questions are:**
  - **Dangerous to whom?**
  - **Danger from where?**

HRI Contexts (non-exhaustive list)

- **Breach – the information is disclosed to unauthorized parties**
- **Law – a legal or regulatory framework defines certain information as protected or prohibited**
- **Intelligence – information gives one party an advantage or influence over another**
- **Vulnerability – a system flaw is exposed that allows attack or compromise**
- **Misinformation – information is untrue or misleading**

Some Current Drivers

- Governance Issues Driving Security
- Security Incidents and Hacking
- Identity Theft and Fraud
- Privacy & Surveillance Concerns
- Critical Infrastructure & National Security
- The Litigious Society

Governance and Security

- What is IT Governance?
- Ethics & Responsibility
- Risks & Controls
- A Growing Culture of Accountability
- Stakeholder and Shareholder Value
- Tying Local Efforts to Larger Strategies

What is IT Governance?

Example: Sarbanes-Oxley (S-OX) Act

Date: 2002

Covers: Corporate governance

Issues:

- **Section 404 addresses internal controls**
- **InfoSec interpreted as covered under Sec 404**
- **Not the only governance law out there**

http://www.aicpa.org/info/sarbanes_oxley_summary.htm

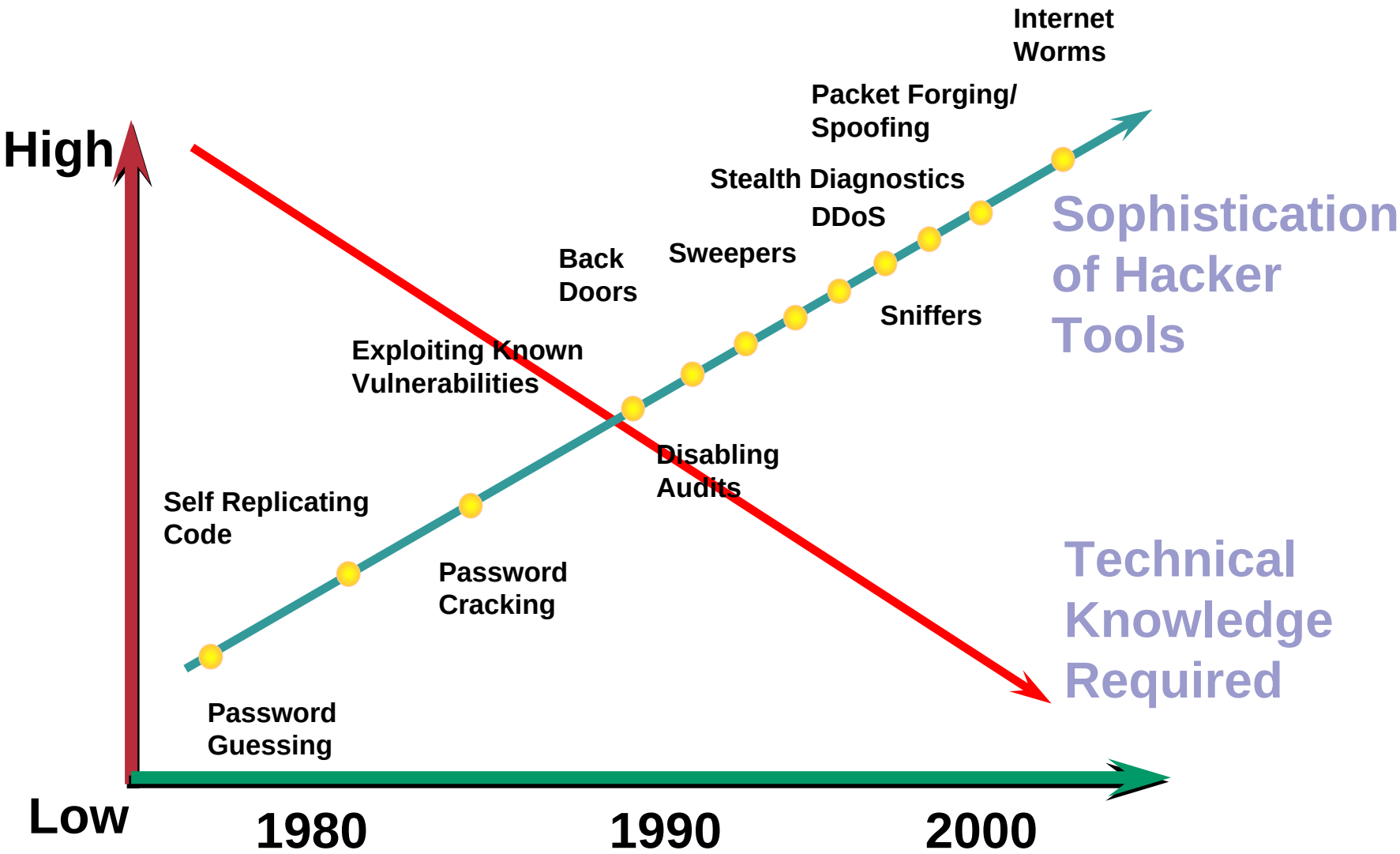
Interpreted S-OX Governance

IF (Corporate governance makes executives and board responsible for all controls in place & their business effectiveness)

AND (IT security provides controls and effectiveness)

THEN (Executive and board management are responsible for IT security)

Security Incidents and Hacking



Identity Theft & Fraud

- 27.3 million victims in USA since 1998
- 9.9 million (36%) in the last year alone
- Institutional losses of $48B in last year
- Consumer losses of $5B in last year
- #1 Consumer fraud complaint in USA
- Internet can enable increased ID theft

Federal Trade Commission

Example: California SB 1386

Date: 2003

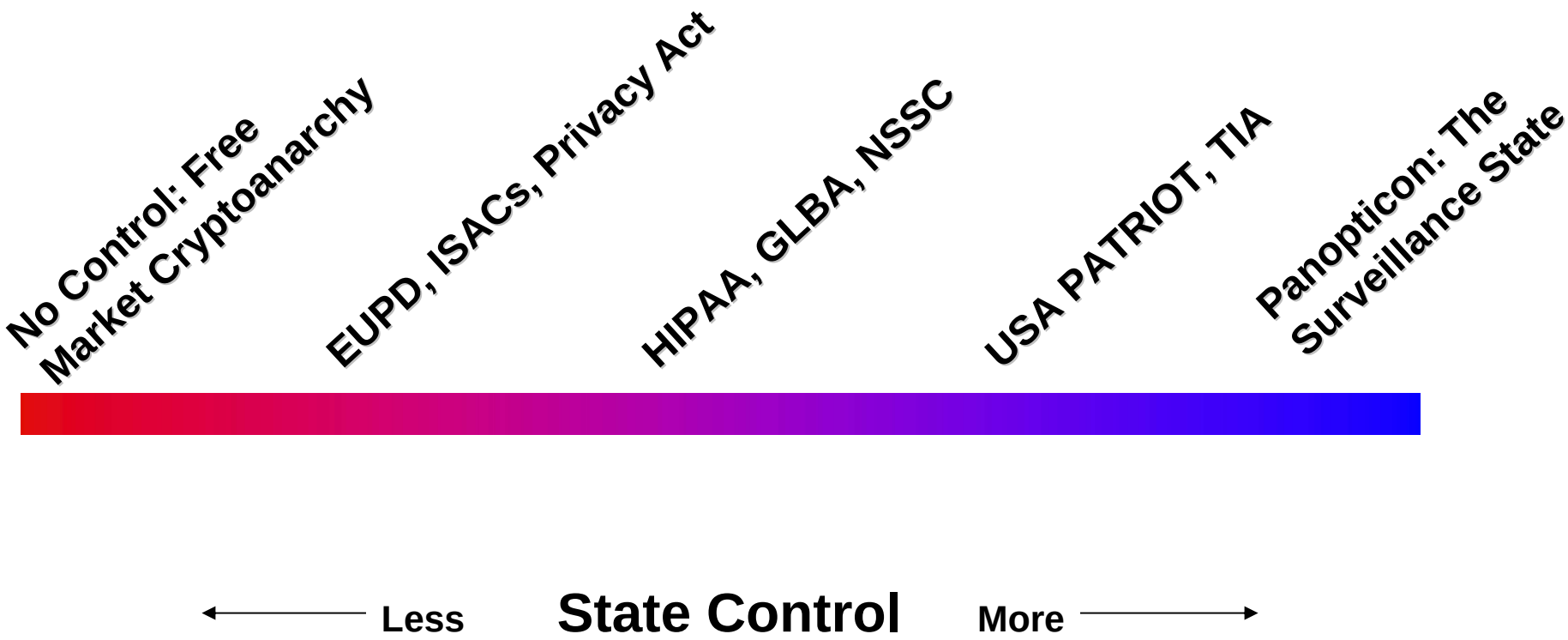
Covers: Anti-ID theft law

Issues:

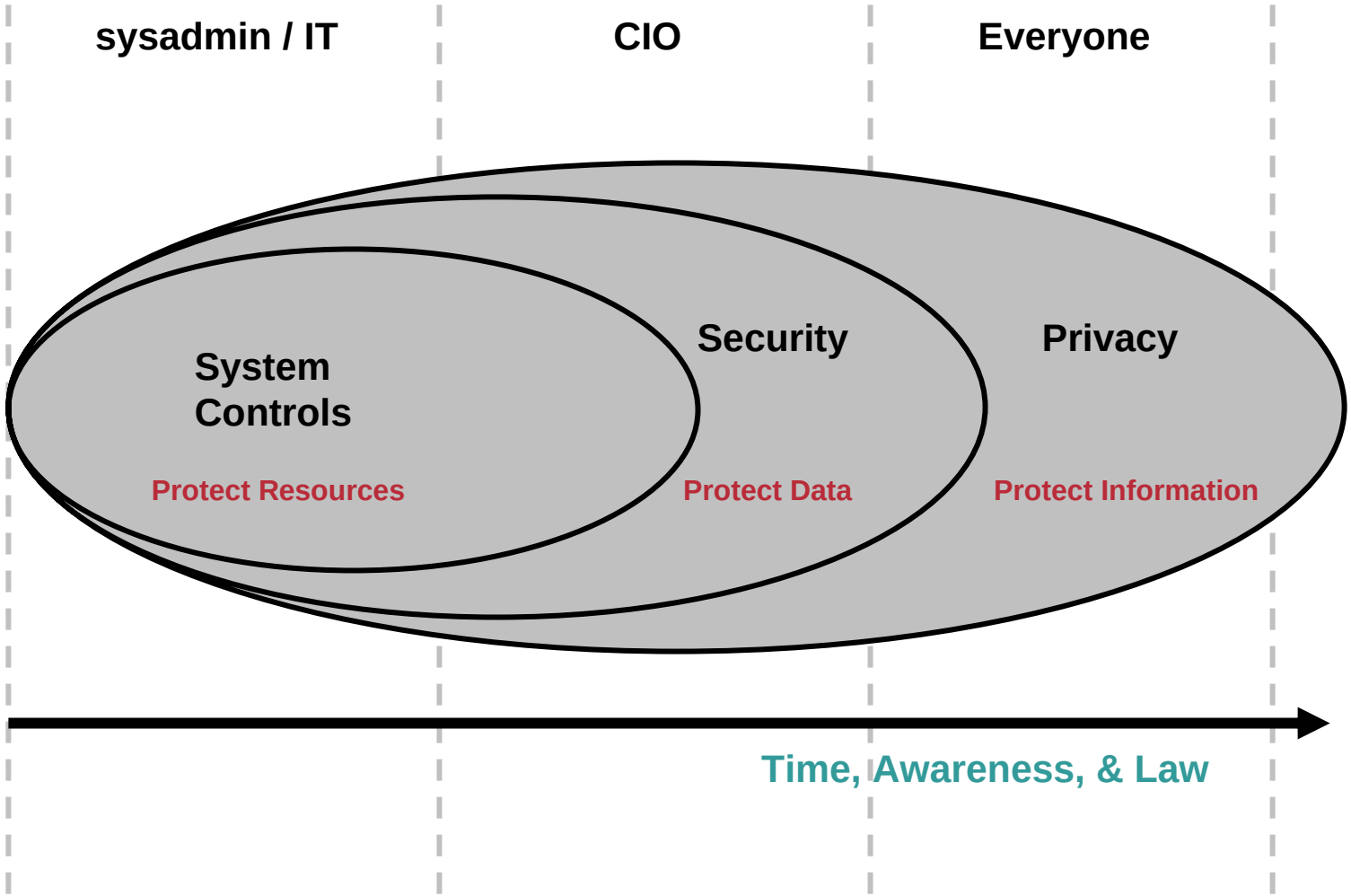
- **Requires organizations holding personal info on California citizens to disclose certain security breaches**
- **Broad potential impact**

http://www.threatfocus.com/security_laws.php?referrer=googlesb1386

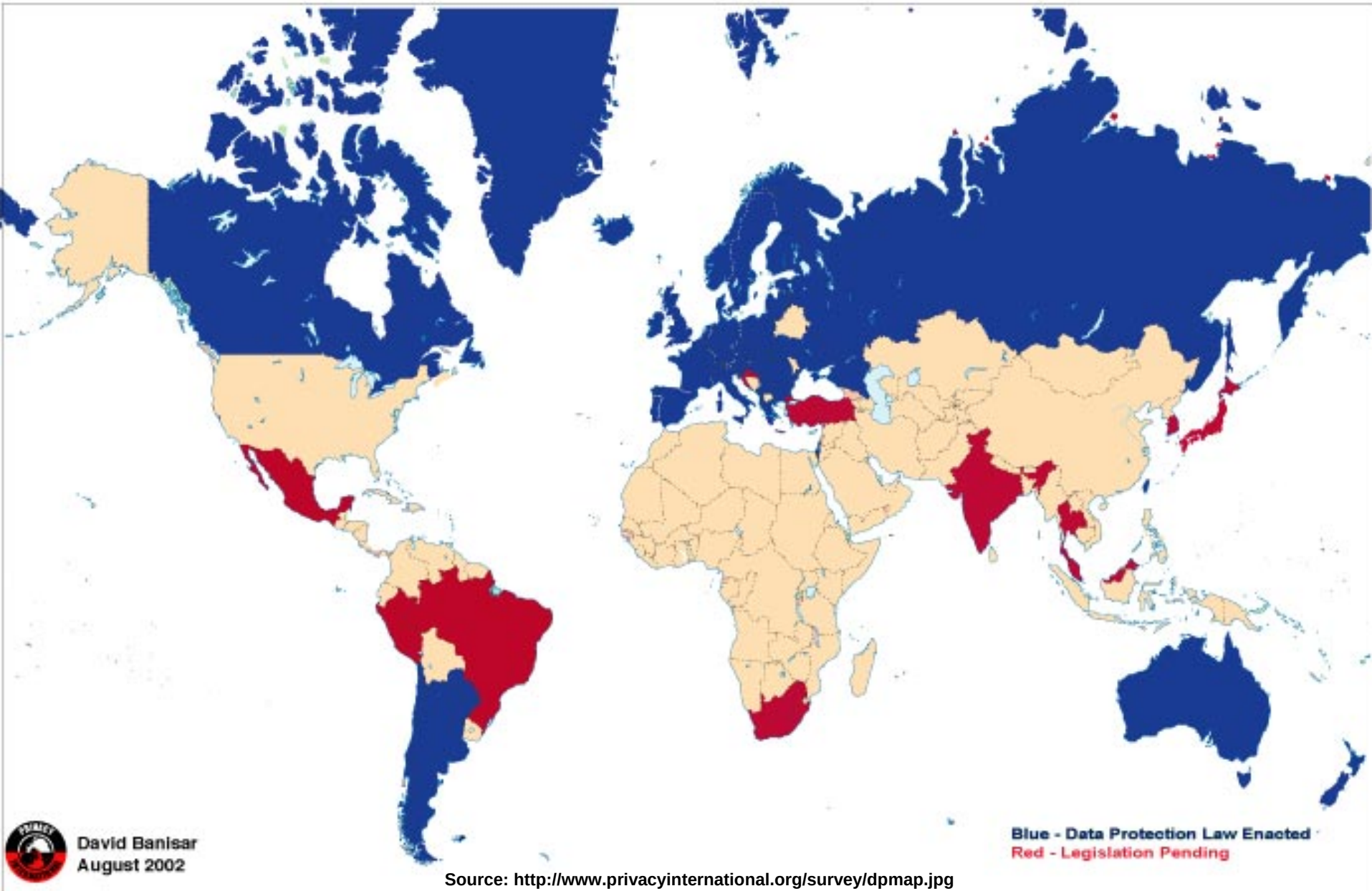
Privacy & Surveillance: A Control Continuum



Security and Privacy Evolution



Data Protection Laws Around the World



Source: http://www.privacyinternational.org/survey/dpmap.jpg

Health Insurance Portability & Accountability Act (HIPAA)

Date: 1996 (Security Regs in 2003)

Covers: Health care data protection

Issues:

- **Often misunderstood or misinterpreted**
- **Regulations are considered ambiguous**
- **Only defines a minimum standard, but many don't know their own state regulations**
- **Lots of marketing FUD**

http://www.hhs.gov/ocr/hipaa/index.html

Gramm-Leach-Bliley Act (GLBA)

Date: 1999

Covers: Financial deregulation and data protection

Issues:

- **More complex than HIPAA**
- **Many regulatory enforcers, rather than one**
- **More sophisticated covered entities**
- **No one set of security guidelines**

http://www.epic.org/privacy/glba/

European Union Directive on Data Protection

Date: 1995

Covers: Omnibus data protection regime

Issues:

- **Affects companies doing business in EU**
- **“Safe Harbor”**
- **Emphasis on trans-border data flow**
- **Modeled elsewhere in the world**

http://www.cdt.org/privacy/eudirective/

Critical Infrastructure & National Security

Lawful Intercept

Cyber-Terrorism

Homeland Security

USA PATRIOT

Espionage

Federal Information Security Management Act (FISMA)

Date: 2002

Covers: Federal Information Systems Security

Issues:

- **Gives NIST more responsibility & authority**
- **Only covers federal systems, but drives others**
- **Tied to Homeland Security efforts**

http://csrc.nist.gov/policies/

USA PATRIOT & USA PATRIOT 2 (proposed)

Date: 2001 / ongoing

Covers: Anti-terrorism, surveillance, national security

Issues:

- **Lots of debate around these laws**
- **Civil libertarians vs. national security angles**
- **Broad implications for electronic communications**

http://www.epic.org/privacy/terrorism/usapatriot/

The Litigious Society

Real Warning Labels:

“Remove child before folding.” (on baby stroller)

“Do not use the Ultradisc2000 as a projectile in a catapult.” (on portable CD player)

“Never iron clothes while they are being worn.” (on household iron)

“DO NOT use soft wax as ear plugs or for any other function that involves insertion into a body cavity.” (on box of birthday candles)

Michigan Lawsuit Abuse Watch (M-LAW) Wacky Labels Contest

Digital Millennium Copyright Act (DMCA)

Date: 1998

Covers: Copyright protection & anti-piracy

Issues:

- **Highly emotional and volatile topic**
- **Vocal and aggressive supporters and detractors**
- **Widespread security & privacy implications for provisions**

http://www.eff.org/IP/DMCA/

“Super DMCA” Laws (enacted & proposed)

Date: Various

Covers: State-level copyright protection

Issues:

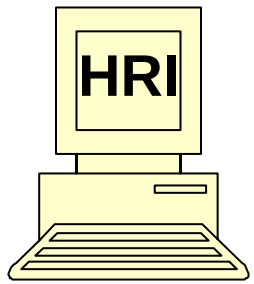
- **In some cases, disturbing components**
- **Interpretations that these laws make things like Network Address Translation illegal**

http://www.freedom-to-tinker.com/superdmca.html

Hey, wait! I'm just the sysadmin!

Breach forces public disclosure...

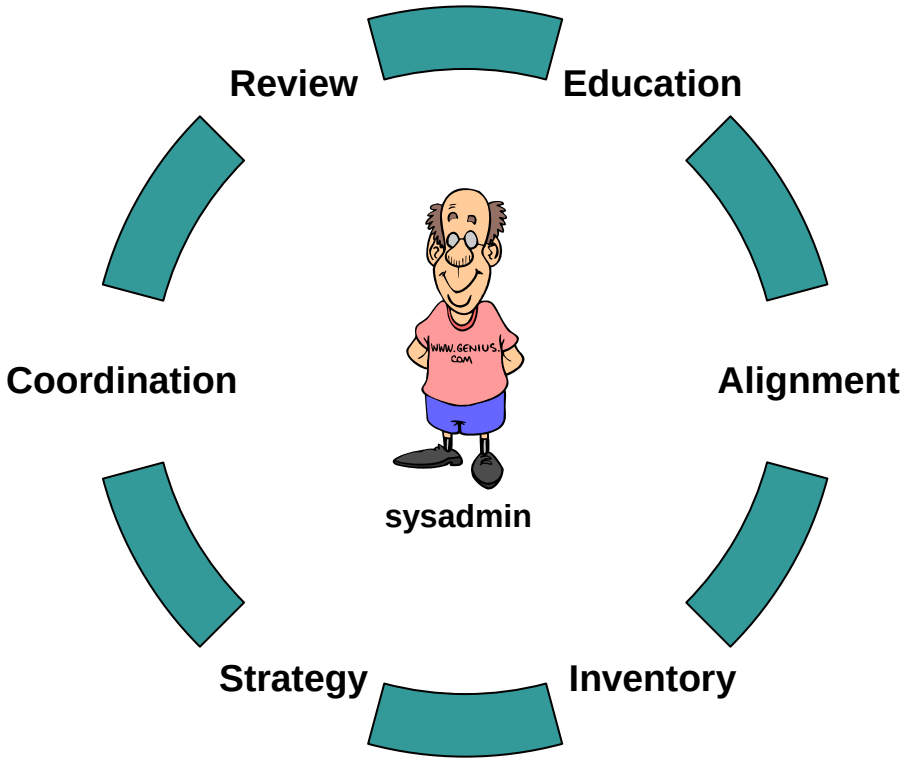
Board subjected to investigation...



User is victim of identity theft...

System is a P2P treasure trove of warez/porn/stolen IP...

An HRI Protection Framework



Education

- **Educate yourself:**
  - **What is my organization's core business?**
  - **What industry regulations am I required to comply with?**
  - **Who is responsible for governance, IT, and security in my organization?**
  - **What is my security posture?**
  - **What is my corporate culture?**
- **You must understand your HRI exposure**

Education

- **Educate others:**
  - **The need to address issues at your level**
  - **How what you do maps to what they do**
  - **The organization's policies, or the need to have them**
  - **The value of testing**
  - **What kind of information you have access to**
- **You must market your protective value**

Alignment

- **Many elements of corporate and IT governance involve aligning technology strategies with business strategies**
  - **How do your systems align with the org as a whole?**
  - **Has anyone ever formally assessed such alignment?**
  - **Work to develop an understanding of where your systems fit into the overall framework**
- **Develop an alignment analysis at whatever level is possible or appropriate**

Inventory

- **Do you know what information exists or may exist on the systems you administer**
  - **Do you process or store sensitive data?**
  - **Do you (or your org) have a panoptic or an private approach to information?**
  - **How is either implemented (do they work?)**
  - **What are the information and system expectations put on you and your users?**
- **Build the inventory at the level possible**

Strategy

- **How will you protect yourself and those who depend on you from an HRI disaster?**
  - **What needs to be done?**
  - **Who do you need to talk to?**
  - **Proactive strategies**
  - **Reactive strategies and incident response**
- **Think globally, act locally**

Coordination

- Using the results of previous phases, begin reaching out
- Management buy-in is critical, but coordination is broader than just management
- Cite the laws and drivers, rather than your opinions
- Do the legwork (at least initially) – “informed networking”
- Make others look good (or promise to)
- Develop SME status (or additional SME status)

Identify Stakeholders

- Board of Directors
- Executive Management
- Security / Data Protection / Audit
- IT Staff
- HR & Legal
- Users
- Vendors & Consultants

Sponsorship, Coordination, & Collaboration

Political
Financial
Application
Presentation
Session
Transport
Network
Data Link
Physical

Key Layer…

The Complete OSI Model

Review

- **Review can be many things:**
  - **Policy level reviews to map strategy with ops**
  - **Information audits**
  - **System and network security testing**
  - **HRI identification – content analysis, information classification schemes**
  - **Strategy reviews that inform subsequent iterations of the HRI framework**
- **HRI is most dangerous to those who ignore the danger**

Going forward…

- **Information concepts will become much more complex**
- **Information protection will be seen as a safety and social issue**
- **Focus put on users & information, not just systems**
- **Broadened responsibility (and liability) for the technologist**
- **Litigation will be as much a driver as regulation**

Conclusions

- You are highly skilled technical specialists…
- …and it won't be good enough.
- Right now this is coming top down, often to the horror of those actually in the trenches…
- Not enough to know your field, you have to know others and how you fit.
- The upside is that knowledge and empowerment are rarely bad things…

Conclusions

- **And trust me – if you think this is all too complex and you can't make an impact…**
- **…most of the people involved are as confused as you think you are.**
- **You can make a difference.**

Questions & Discussion