Managing Cyber Risk for State Governments

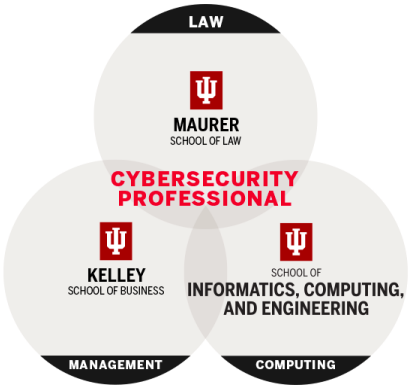
THE GRIFFITH™
INSURANCE EDUCATION
FOUNDATION

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

INDIANA UNIVERSITY

IU Cybersecurity Risk Management Program

- Multidisciplinary (Law, Secure Computing, & Business)
- Built on IU's Cybersecurity Certificates
- Applied Cybersecurity Risk Management Capstone
- Online courses available
- Size: 80+ (Fall 2019)
- Advisory Council



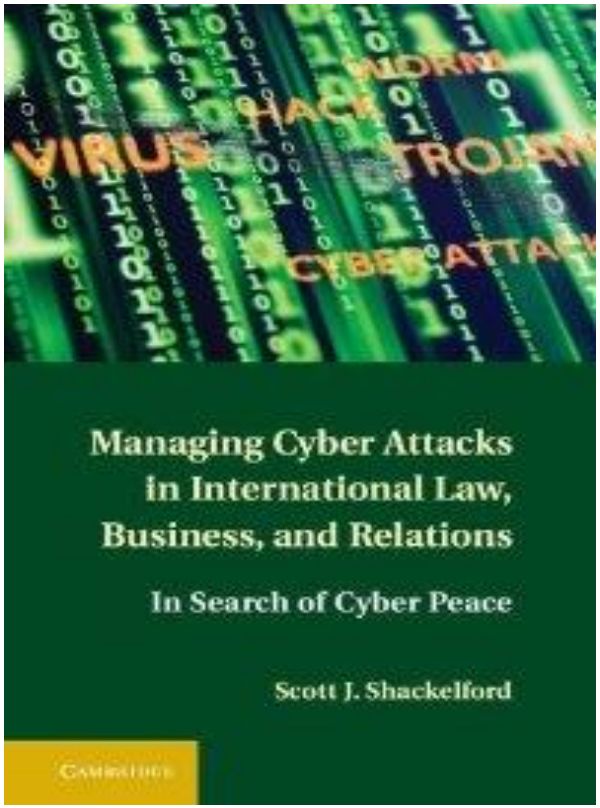
Ostrom Workshop Program on Cybersecurity & Internet Governance

- **Goal**: Applying polycentric principles to cybersecurity challenges
- **Insight**: Leverage nested governance structures that may be small in scope and scale, but start somewhere!
- **Literatures**: Regime complex, linkages, network effects, institutional analysis
- **Potential Issues**:
  - Fragmentation
  - Gridlock
  - Ethical and Political Pitfalls

Ostrom Workshop

Objectives

1. **Regulating Cyberspace**
   - A. What is cyberspace?
   - B. Theories of Regulation & the Role of Insurance
2. **Breaking Down the Cyber Threat**
3. **Managing Cyber Attacks**
   - A. Identifying Threats
   - B. Regulatory Approaches and Examples
   - C. Cybersecurity Best Practices
4. **The Global Dimension**
   - A. Comparative Cyber Risk Mitigation Strategies
   - B. International Law & Attribution



Introductory Example

Background: *In May 2011, Sony's PlayStation network was attacked, and hackers reportedly compromised more than 100 million gamers' names, addresses, emails, user names, and passwords. The attack may ultimately cost Sony between $1 and $2 billion directly, and potentially billions more indirectly because of reputational harm as well as costs to consumers and credit card companies. A legal battle has been brewing that includes more than 50 class action lawsuits over who should pay.*

Discuss:

1: Who should pay for identify theft?

2: What role should insurance play?

3: Should the U.S. favor a more voluntary or regulatory approach to regulating data breaches and enhancing cybersecurity?

4: How does this episode color Sony's response to the 2014 cyber attacks? What could Sony have done better?

Introductory Example #2

Spotlight: The 2012 South Carolina DoR Data Breach

***Background**:* On August 13, 2012, an employee at the South Carolina Department of Revenue (SCDOR) received an email with a link embedded in the message. She clicked on the link and, in doing so, unknowingly downloaded malware onto her work computer in the state government. Two weeks later, someone used her username and password—presumably collected by means of that malware program—to log into her work account remotely. It was the first step in what would turn out to be a month-long operation to steal more than three-and-a-half million tax records dating back as far as 1998 and affecting more than 75 percent of the population of South Carolina.

***Discuss*:**

1. Why are tax returns potentially more valuable to cyber criminals than credit card numbers? What other types of information might be similarly prized?
2. How could the state have avoided this breach, or failing that, at least made it harder on the hackers to be successful?

Discussion Questions

- Under what circumstances are governments justified in regulating cyberspace? Is there a cybersecurity market failure?
- What role should cyber risk insurance play as part of cyber risk mitigation?
- What is the "Internet of Things," and how might it be secured? What role is there for state government?
- Are we now in a cyber war? What hope is there for cyber peace?

Cyberspace

	Tangibles		Intangibles					Network Related			
	ICT IT[1]	HW	Information[2]	Activities	Application Service	Social Human	Virtual	Internet	Network	Interconnectedness	Communication
Oxford Dictionary							✓	✓			✓
Australia*	✓	⊙	⊙								
Canada	✓	⊙	✓		✓	✓	✓		✓	✓	
Germany	✓	⊙	✓				✓	✓	✓	✓	
The Netherlands*	✓	⊙	⊙								
New Zealand	✓	✓							✓	✓	✓
UK			✓	✓	✓	✓	⊙	✓	✓		✓
USA	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
EU		✓	✓				✓				
ISO		✓	✓	✓	✓	✓	✓	✓	✓	✓	
ITU		✓	✓		✓	✓	✓	✓	✓	✓	

[1]Hardware encompasses items like: computer, PC, procesor, controller, etc.
[2]Information includes signalling (i.e., communication between processes and/or devices) but also the content of the exchange.
√ The definition explicitly references this element
⊙ the definition implicitly references this element
* Derived definition. There was no direct definition of cyberspace so its meaning was derived from other definition (most commonly from cyber security)

True/False Cyber Quiz

1. It is estimated that 90% of successful breaches use the most basic techniques, including social engineering.
2. Most cyber attacks are not discovered immediately; in fact, 85% of cyber attacks take on average at least 5 months for the organization to find.
3. The majority of organizations only find out they have been breached after they have been notified by a third party.
4. Over $1 trillion is lost to cyber criminals globally each year, whereas ransomware can be purchased for as little as $400.
5. More than fifty percent of public-sector organizations now carry cyber risk insurance.

Defining the Cyber Threat

To Companies

- Theft of IP is **Costly** – by some estimates (McAfee) more than $400 billion annually
- **Widespread** – at least 19 million people in 120 nations
- **Easy** –more than 30,000 sites with malware available for download
- **Expanding** – Internet of (Every)thing

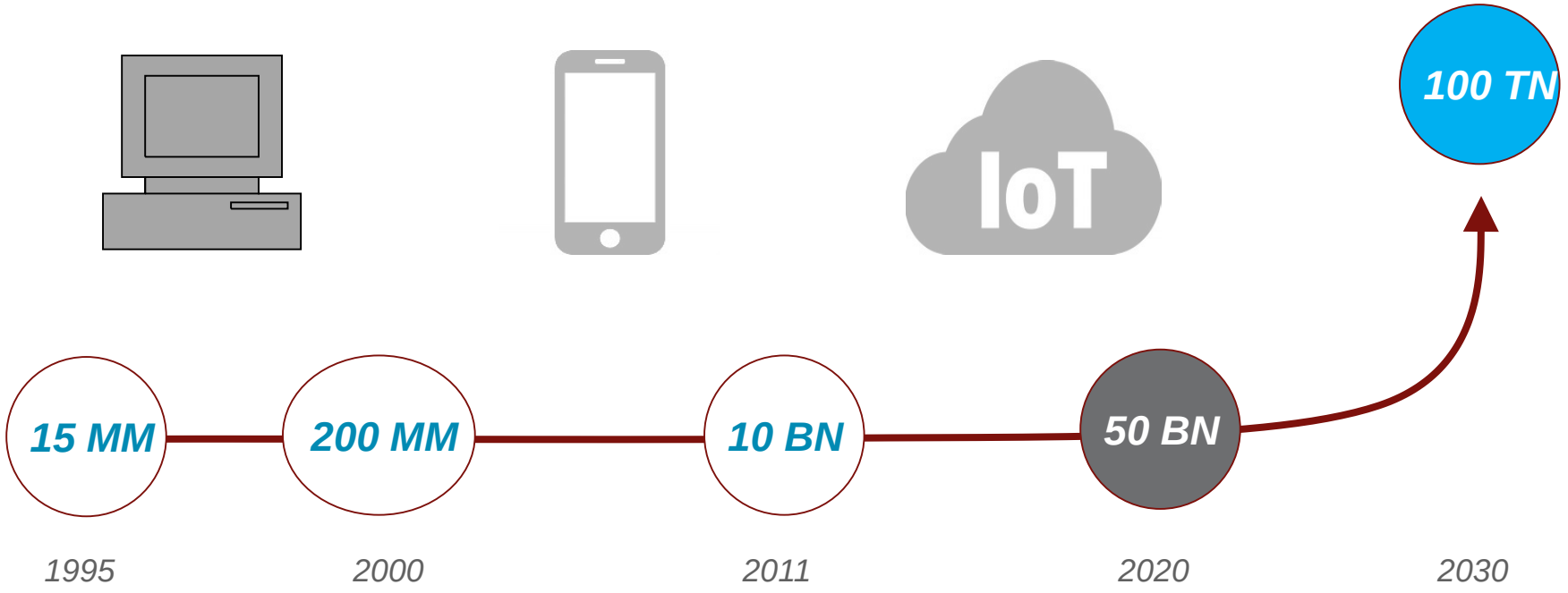
To Countries

- Fear of "Electronic Pearl Harbor" (overblown?)
- Protecting critical national infrastructure

*Source: KAL's Cartoon, Economist, May 7, 2009

The Internet of Everything – Exploring Technical Vulnerabilities & Internet Governance Lessons

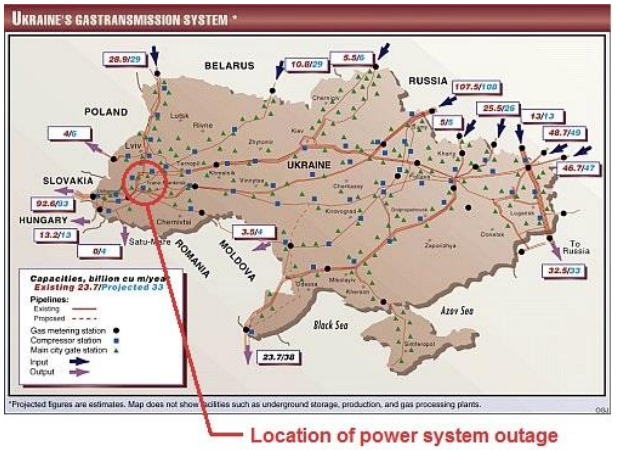
The number of connected objects is rising exponentially – 50 billion+ connected objects expected by 2020



Source: Oliver Wyman analysis

Developments & Strategy

- New Types of Attacks (Ukraine Grid (2015/16))
- Governments have learned that it is often easier to steal sensitive information via the Internet than in-person
  - Anonymous
  - Cost-Effective
  - Rapid Results
  - Economies of Scale
  - Low Risk, High Reward

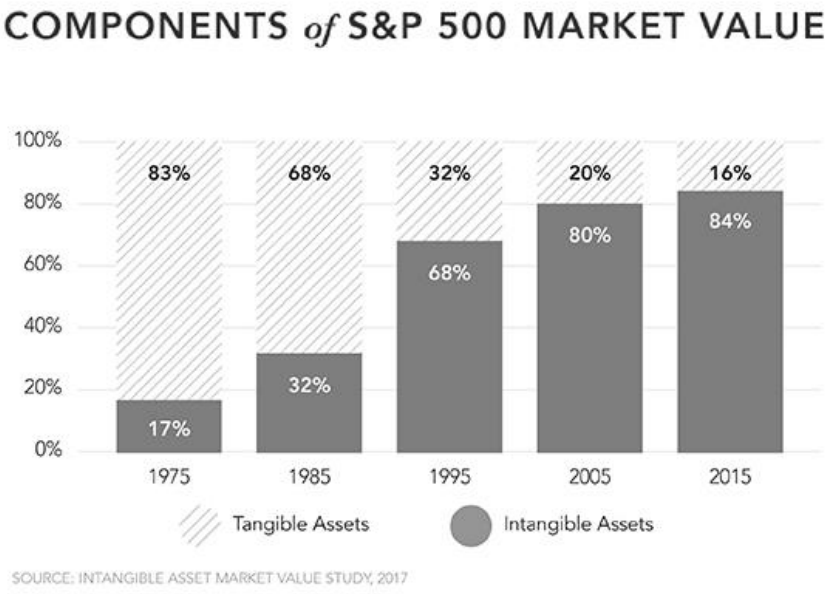


- Corporate IT security departments are outnumbered
- One successful intrusion can steal gigabytes (or more) of information worth millions of dollars (or more)

Unpacking the "Cyber Threat"

- Cyber War
- Cybercrime
  - Many Types
  - True Extent Unknown
  - Global Nature
  - Response
- Cyber Espionage
  - Legal "black hole"
  - Cost
- Cyber Terrorism
  - Ransomware
  - Why relatively rare?
- New Cyberwarfare

*Source: The War Room



*Source: McAfee In the Dark (2010)

“[T]he cyber threat cannot be eliminated; rather, cyber risk must be managed.”

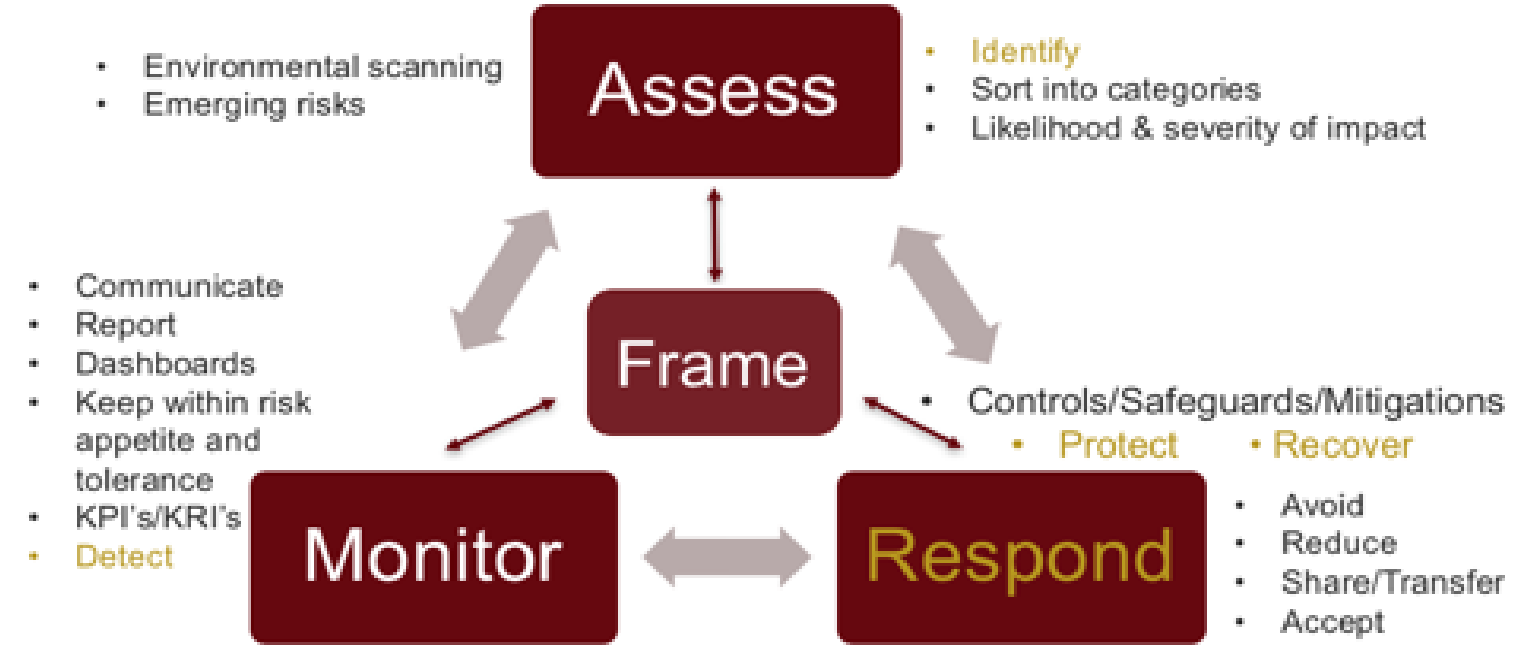
Director of National Intelligence James R. Clapper
Worldwide Cyber Threats Testimony, Sep. 10, 2015

Definition of ERM

- ✓ A process
- ✓ Effected by an entity's **board of directors**, management, and other personnel
- ✓ **Applied in strategy-setting** and across the enterprise
- ✓ Designed to identify potential events that may affect the entity and manage risk to be within its risk appetite
- ✓ To provide reasonable assurance regarding the achievement of entity objectives.

NIST SP 800-30
Risk Management Process

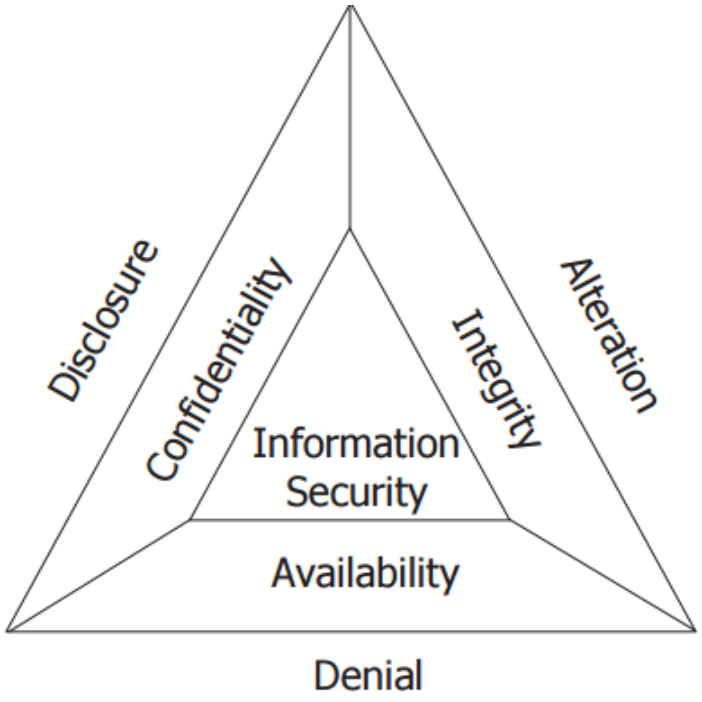
Revision 1, Page 4
With annotations by mbl



Examples of IT-Related ERM Risks

- Loss of external network
- Loss of internal wired core network
- Inability to recruit and retain sufficient IT personnel
- Data breach involving PHI, SSN, CC, or bank data
- Failure to keep pace with the advancing technological business support tools
- Loss of analog system communications hub
- Loss of email system
- Disruption of middleware software

CIA v. DAD

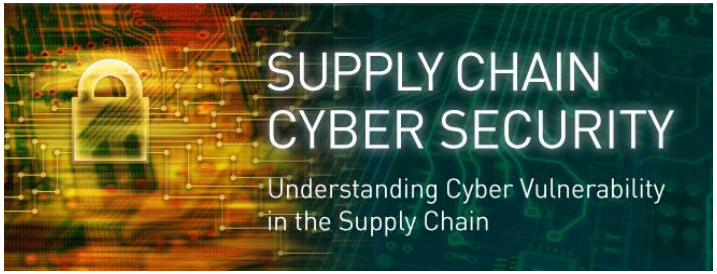


- **CIA** (Confidentiality, Integrity, Availability): Goal is to implement security best practices (Defenders)
- **DAD** (Disclosure, Alteration, Denial): Goal is to defeat security of an organization (Attackers)

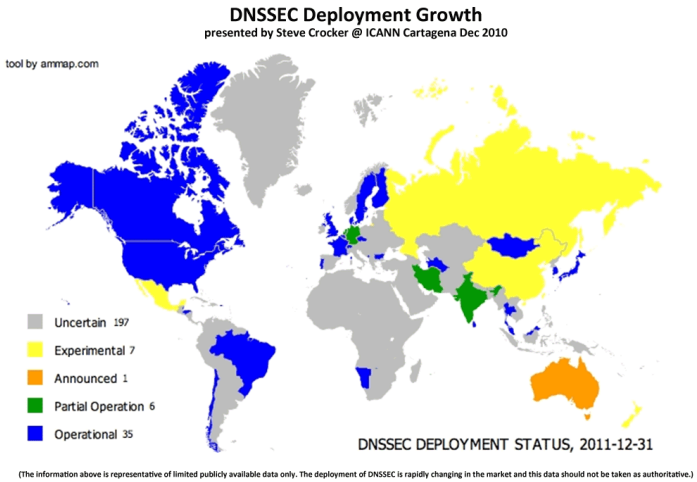
Managing Cyber Attacks

Technical Vulnerabilities

- Hardware
  - Secure Supply Chains
  - “Trust but Verify”
- Protocols
  - Ex: DNS
  - Importance of DNSSEC
- Code
  - Improving Accountability
  - Liability Issues
- Users



*Source: *www.aronsonblogs.com*



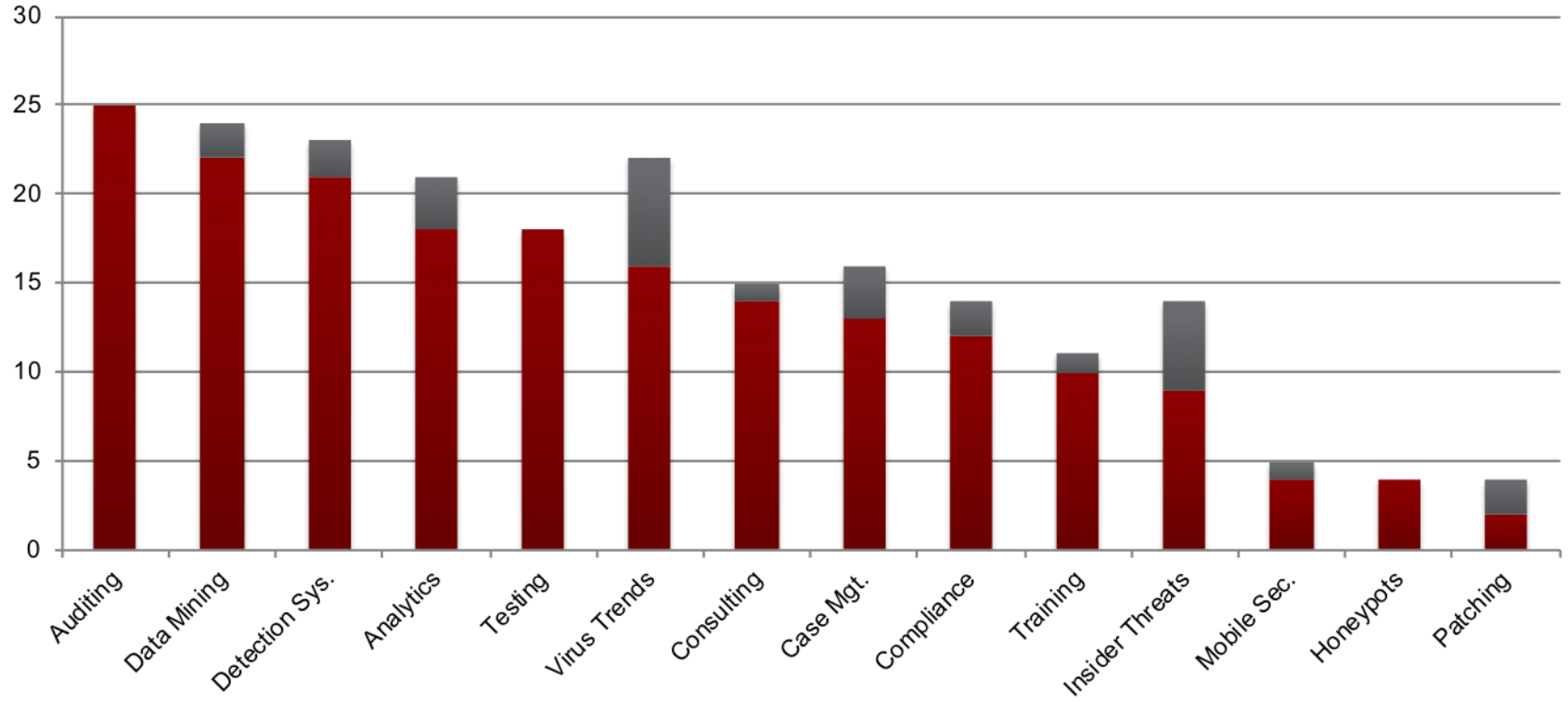
*Source: *www.techbyte.pl*

Private-Sector Cybersecurity Best Practices

- **Summary**: Be *proactive* and invest in built-in cybersecurity best practices from the inception of a project.
- **Technology**
  - Encrypt Data (at rest and in transit)
  - Biometrics & Deep Packet Inspection
- **Investments**
  - Average: >10-15% of IT budgets
  - Cybersecurity as CSR
- **Organization**
  - CISO Savings
  - Audit Training Programs & Penetration Testing

*Source: www.wizilegal.com

Snapshot of "Proactive" Cybersecurity Best Practices



Defining ‘Reasonable’ Cybersecurity

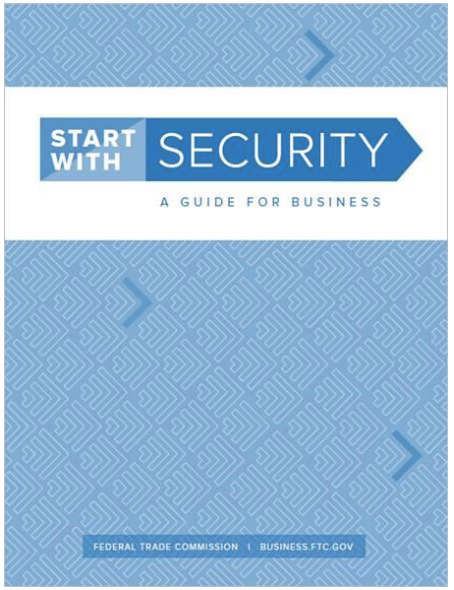
Negligence and the NIST Cybersecurity Framework

*Source: *welivesecurity.com*

- **2013 State of the Union Address**
  - Focus on cyber threats to nation's critical infrastructure
- **Executive Order 13636: Improving Critical Infrastructure Cybersecurity**
  - Increase information sharing
  - Ensure privacy and civil liberties protections
  - Develop a voluntary Cybersecurity Framework

FTC Cybersecurity Best Practices

1. Start with Security
2. Compartmentalize Access to Data
3. Require Secure Passwords & Authentication
4. Store/Transmit Personal Info Securely
5. Segment & Dynamically Monitor Networks
6. Secure Remote Access
7. Cybersecurity-Awareness Training
8. Ensure Security of Service Providers
9. Regularly Update Security Practices
10. Secure Paper, Physical Media & Hardware



State-Level Cybersecurity Laws

Type of State Law	Coverage	Description
Hacking, Unauthorized Access, Computer Trespass, Viruses, Malware	All 50 States	All fifty states have enacted laws that generally prohibit actions that interfere with computers, systems, programs, or networks.
Data Breach Notification Laws	All 50 States	
Anti-Phishing Laws	23 States: Alabama, Arkansas, Arizona, California, Connecticut, Florida, Georgia, Illinois, Kentucky, Louisiana, Michigan, Minnesota, Montana, New Mexico, New York, Oklahoma, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia, Washington, and Guam	A total of twenty-three states and Guam have enacted laws targeting phishing schemes. Many other states have laws concerning deceptive practices or identity theft that may also apply to phishing crimes.
Anti-Denial of Service/DDoS Laws	25 States: Alabama, Arizona, Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Mississippi, Missouri, Nevada, New Hampshire, North Carolina, Ohio, Oklahoma, Pennsylvania, South Carolina, Tennessee, Virginia, Washington, West Virginia, and Wyoming	
Anti-Spyware Laws	20 States: Alaska, Arizona, Arkansas, California, Georgia, Hawaii, Illinois, Indiana, Iowa, Louisiana, Nevada, New Hampshire, New York, Pennsylvania, Rhode Island, Texas, Utah, Virginia, Washington, Wyoming, Guam, and Puerto Rico	There are twenty states and two U.S. territories have laws expressly prohibiting use of spyware. Other state laws against deceptive practices, identity theft, or computer crimes in general may be applicable to crimes involving spyware.
Anti-Ransomware Laws/Computer Extortion Laws	5 States: California, Michigan, Connecticut, Texas, and Wyoming	Currently four states have statutes that address ransomware, or computer extortion; however, other state laws prohibiting malware and computer trespass may be used to prosecute these crimes as well.

GDPR Operational Impacts & NIS Directive

1. Cybersecurity & Data Breach Requirements
2. Mandatory Data Protection Officer
3. Consent
4. Cross-Border Data Transfers
5. Profiling
6. Data Portability
7. Vendor Management
8. Pseudonymization
9. Codes of Conduct & Certifications
10. Consequences of Non-Compliance

**Source: IAPP*

Highlights of China Cybersecurity Law

**Source: KPMG*

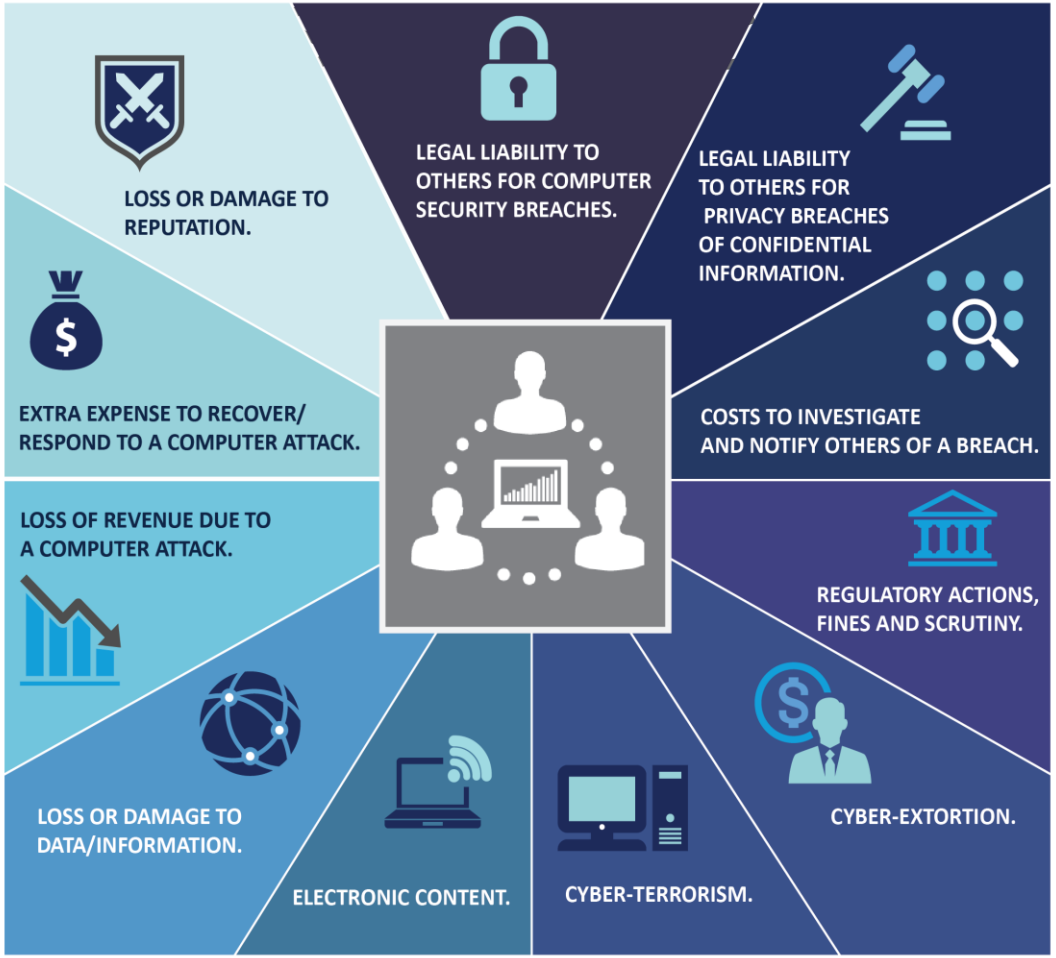
Cyber Risk Insurance

Cyber Risk Insurance

- **Growth of Market**
  - 2003: Approx. $100m
  - 2016: Approx. $1.3b
- **Benefits**
  - Lifeline
  - Sample Plan
- **Costs**
  - Reactive
  - Hard to Quantify Risk

*Source: *Betterley Risk*

Cyber Insurance



First Party

- Cyber Event Management
- Data Restoration
- Network Business Interruption
- Cyber Extortion

Third Party

- Privacy Liability
- Network Security Liability
- Privacy Regulatory Defense Costs
- Media Liability

Cyber Risk Factors

- Revenue
- Industry
- Geographic Footprint
- Amount/Storage of Private PII/PHI
- Supply Chain Risks
- Third-Party Risk Assessments
- Governance

Why are Organizations Buying Cyber Risk Insurance?

Risk Transfer

- *Escalation of cyber attacks impacting operations.*
- *A top priority on the corporate risk agenda.*
- *Regulatory requirements/SEC cyber disclosure guidance.*
- *Litigation and contractual obligations.*
- *Part of comprehensive cyber risk management strategy.*
- *Coverage expansion, favorable pricing and more service offerings.*

Cyber Risk Insurance Checklist

- Both first *and* third party **coverage**?
  - Notification costs?
  - Crisis management?
  - Call centers?
  - Credit monitoring?

- What **exclusions** are included? How are they defined?

Cyber Risk Insurance Simulation

The State of Franklin has a cyber risk insurance policy with TrustUs, a leading insurance carrier. Following a ransomware attack, Franklin's policymakers are presented with a series of options and must choose which policy best meets their cyber risk mitigation needs, which includes the need for a long duration of coverage as well as coverage for third parties that may be harmed due to an inability to access the insured's system.

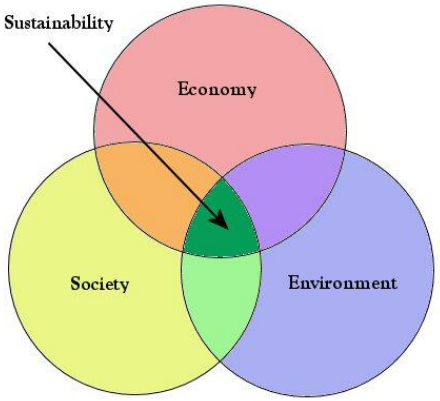
Third Party Coverage: Defense Costs and Third Party Damages	
Policy A	**Policy B**
Covers damages, judgments, settlements, and interest that the insured is legally obligated to pay, resulting from a written demand, lawsuit, or regulatory action, alleging • a failure or violation of the security of a computer system or a failure to protect confidential information, • failure to disclose a failure to protect confidential information in violation of disclosure laws, or • violation of any privacy statute. Available Media Policy covers damages and defense costs where insurable by the applicable law for any act, error, omission, negligent supervision of an employee (including the broadcast or distribution) of media content (TV/internet broadcasts, publications) by the insured that results in: • Copyright, trademark, domain name infringement • Plagarism, theft, misappropriation • Invasion of rights of privacy or publicity • Defamation/libel/slander • Trespass, eavesdropping • Infliction of emotional distress • Loss because a third party acts upon or makes a decision based upon the disseminated materials	Covers damages, judgments, settlements, and interest that the insured is legally obligated to pay, resulting from a written demand, lawsuit, alleging: • **Disclosure Injury** (an injury resulting from unauthorized use of confidential information that occurs during the policy period and results from a cyber attack or a hacker). • **Reputational Injury** (injury sustained for disparagement of an organizations products or services, libel, slander, violation of rights of privacy or publicity as a result of the electronic display, transmission, or dissemination of information through the insured's system.) • **Content Injury** (infringement of a trademark, copyright, name of product, service or organization, or the title of an artistic or literary work) • **Conduit Injury** (third party's loss of use of its own system caused by cyber attack) • **Impaired Access Injury** (injury from third party's inability to access the insured's system)

Insurance Hot Topics & Trends

- Bodily Injury and Property Damage
- Reputational Loss
- IoT coverage
- Supply Chain Risks
- Blockchain & Crypto
- Regulatory Environment

Other Options for Bottom-Up Cyber Risk Mitigation

- Tragedy of the Cyber Commons?
- Some Applicable Tools:
  - Integrated Reporting
  - Certificate Programs
- State Experimentation
  - *Should your state have an **ISAC**? CERTs?*
  - *What about **clinical collaborations**?*
  - *Grow the state **cyber corps** and **red teams**?*



*Source: *www.keepoklahomabeautiful.com*

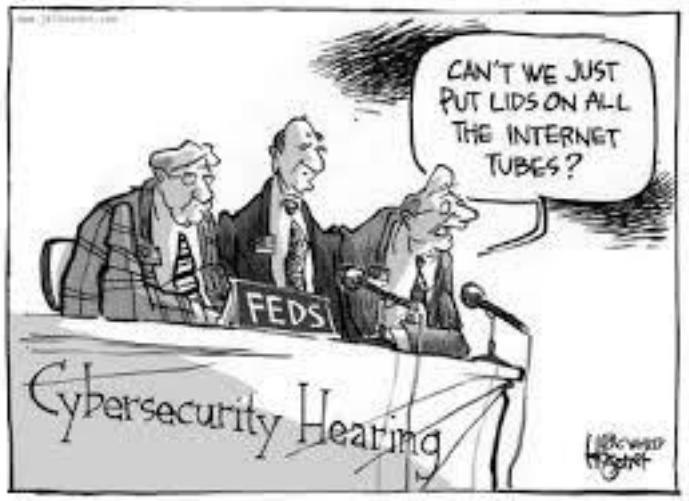
Additional State-Based Cybersecurity Reform Options

- *Should your state sponsor a **public bug bounty** program? What about training for **critical infrastructure providers, penetration testing,** or **internal phishing**?*
- *What sorts of **cybersecurity awareness raising** activities are on offer? How are they targeted? What about school corporations?*
- *Is it time to update your state's **data breach notification** law?*
- *What about mandating **NIST Framework compliance**?*

Appendix

U.S. Cybersecurity Law Roadmap

- FTC Act Section 5
- State Data Breach, Cybersecurity, and Consumer Privacy Laws
- Cybersecurity Litigation
  - Standing
  - Negligence
  - Negligent Misrepresentation
  - Breach of Contract
  - Breach of Implied Warranty
  - Invasion of Privacy
  - Unjust Enrichment
  - State Consumer Protection
  - Class Actions
- Corporate Governance (SEC, CFIUS)
- Federal Sector-Specific Laws



FTC Unfairness Policy Statement

1. Injury must be **substantial**
2. Not be outweighed by **offsetting consumer or competitive benefits**
3. Injury must be one which consumers could not reasonably have **avoided**

FTC Example – Wyndham Hotels

In 2008 and 2009, hackers penetrated the networks of Wyndham Worldwide Corp. and stole the PII of hundreds of thousands of customers leading to more than $10 million in fraudulent charges. Among the documented security failures that the FTC found were:

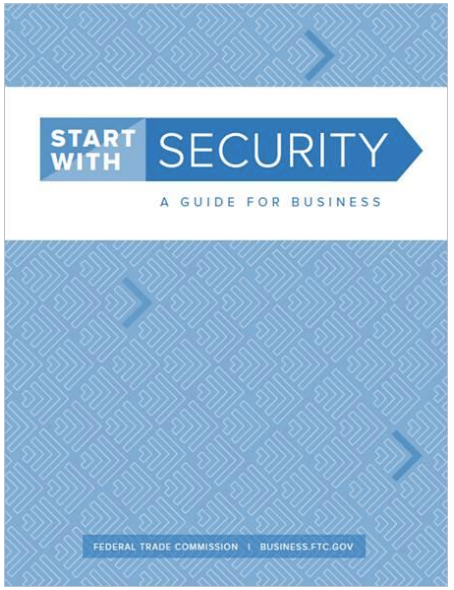
- Storing credit card data in clear text
- Allowing simple passwords
- Not using firewalls
- Failing to police the practices of vendors/partners

WYNDHAM HOTEL GROUP

Wyndham countered that the FTC did not have authority to bring cybersecurity-related actions against firms. What happened next? How could this case have turned out differently? What would have been the consequences?

FTC Cybersecurity Best Practices

1. Start with Security
2. Compartmentalize Access to Data
3. Require Secure Passwords & Authentication
4. Store/Transmit Personal Info Securely
5. Segment & Dynamically Monitor Networks
6. Secure Remote Access
7. Cybersecurity-Awareness Training
8. Ensure Security of Service Providers
9. Regularly Update Security Practices
10. Secure Paper, Physical Media & Hardware



Core Cybersecurity Litigation Questions

- *What are we protecting?* [**Intellectual Property/CI**]
- *What can we do to protect it legally?* [**Contracts**]
- *What happens when things go wrong?* [**Torts**]
- *What are the fiduciary duties for managers to enhance cybersecurity?* [**Agency**]
- *How does privacy law relate to cybersecurity?* [**Privacy**]
- *How big of a problem are cyber attacks really, and what are the best practices to mitigate the threat?* [**Management**]
- *How does the U.S. approach to cybersecurity compare to other global players?* [**International law**]

Contracts Hot Topics

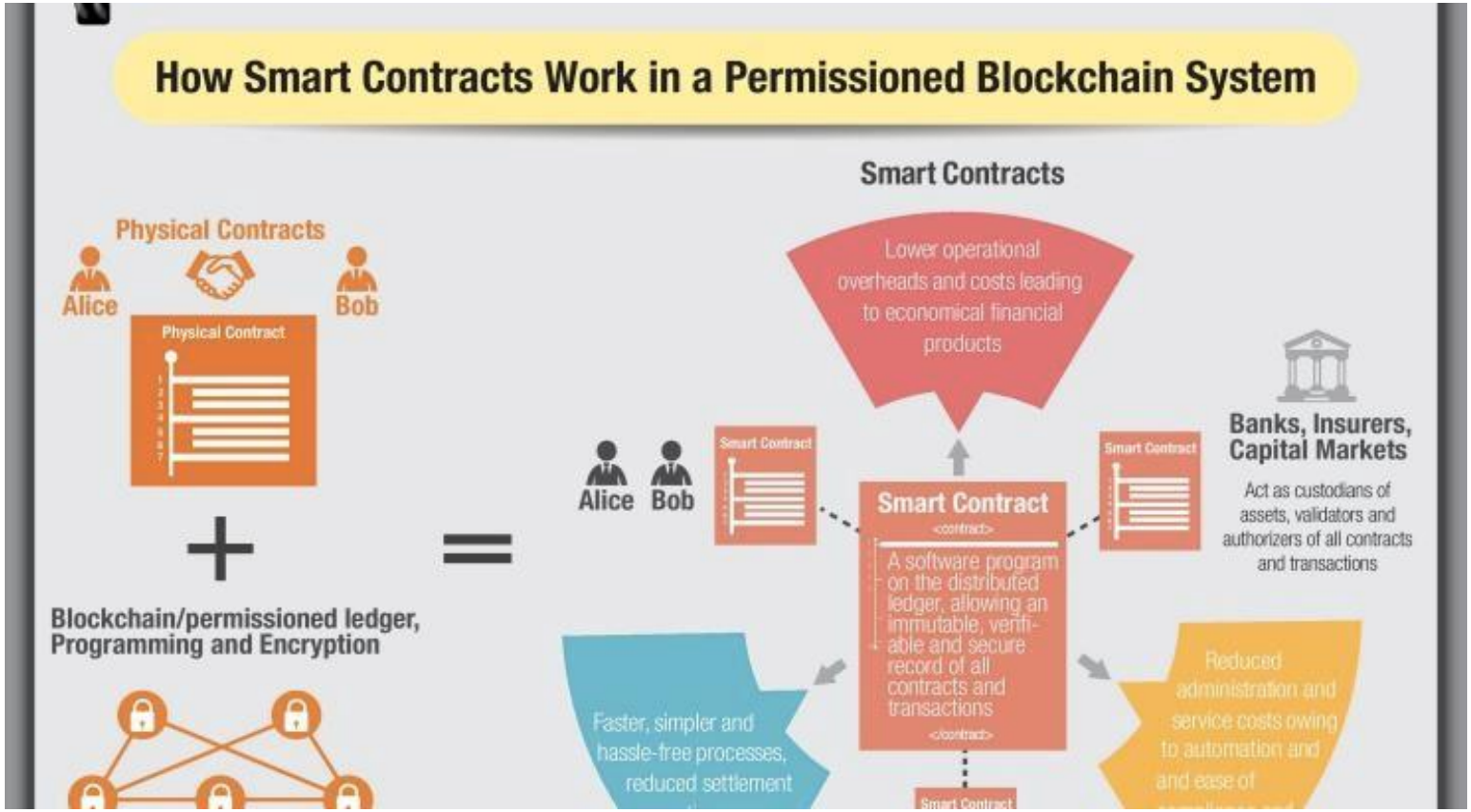
Model Cybersecurity Contracts Clauses

- **Examples**:
  - The Contractor must: (a) do all things that a reasonable and prudent entity would do to ensure that all Customer Data is protected at all times from unauthorised access or use by a third party or misuse, damage or destruction by any person;
  - (b) provide protective measures for the Customer Data that are no less rigorous than accepted industry standards and commensurate with the consequences and probability of unauthorised access to, or use, misuse or loss of, the Customer Data;
- For the **Full List**, Click Here

Smart Contracts – Regulating Blockchain

- Rise of Bitcoin
- Defining a Blockchain
- Potential to revolutionize contracting
- Benefits/Drawbacks over Traditional Systems
- Role for States?

How Does This Work?



Torts Hot Topics

Categories of Torts

- **Intentional** – "[T]he desire to cause certain consequences or the substantial certainty that those consequences will result"
- **Recklessness** – "[A] conscious indifference to a known or substantial risk of harm"
- **Negligence** – "Failure to use reasonable care, with harm to another party occurring as a result"
- **Strict liability** – "Liability irrespective of fault"

What are the elements of negligence?

1. Defendant owed a **duty of reasonable care** to the Plaintiff,
2. Defendant **breached** this duty of reasonable care, and
3. Defendant's breach of duty was **actual and proximate cause** of Plaintiff's **injury**

Note:

- **Examples**: medial malpractice, driving drunk, etc.
- **Defenses**: comparative/contributory negligence

Negligence Example: TJ Hooper, 60 F. 2d 737 (2d Cir. 1932)

- Facts
- Issue
- Holding
- Analysis
- Implication for Cybersecurity
  - Firewalls? Intrusion Detection Systems?
  - Biometrics? Regulator Penetration Testing?

Negligence and the NIST Cybersecurity Framework

*Source: *welivesecurity.com*

- **2013 State of the Union Address**
  - Focus on cyber threats to nation's critical infrastructure
- **Executive Order 13636: Improving Critical Infrastructure Cybersecurity**
  - Increase information sharing
  - Ensure privacy and civil liberties protections
  - Develop a voluntary Cybersecurity Framework

Fiduciary Duties

Cybersecurity & Fiduciary Duties

- **Review**:
  - What is agency law?
  - What are the fiduciary duties?
  - What types of authority exist in an agency relationship?

- **Application to Cybersecuirty**:
  - What is a director's fiduciary obligation when it comes to cybersecurity?
  - Should states be engaged in cybersecurity education to better inform managers?

Fiduciary Duties Example

Breaches ‘R Us is a publicly traded and engaged in the business of selling green technologies worldwide. Breaches network is hacked by an outside party who obtains customer information and technical documents related to a more efficient solar cell. Following the public disclosure of the cyber attack, Breaches share price drops by 9 percent within five days, response costs exceed $10 million, and several consumer class action law suits are filed. Shortly after the breach, several large pension funds initiate derivative litigation against the board of directors alleging that the loss in shareholder value and harm to the company was a direct result of the directors’ failure to proactively address cybersecurity. What will likely happen next?

**Source: Cybersecurity and the board of directors: avoiding personal liability – Reuters*

Breach of Privacy

Invasion of Privacy

- **What is "Privacy"?**
- **Employee Privacy**
  - Polygraph?
  - Drug testing?
  - Employee searches and monitoring?
- **Federal Regulation** (non-comprehensive)
  - *Old Statutes*
    - 1970 Fair Credit Reporting Act
    - 1974 Privacy Act
    - 1974 Family Educational Rights and Privacy Act
  - *New Statutes*
    - 1996 HIPAA
    - 1999 Gramm-Leach-Bliley Financial Services Modernization Act
    - 2002 CA Personal Data Protection Law (SB1386)

Regulating Privacy

- **Recent Developments**
  - FCC Broadband Consumer Privacy Rules (CRA)
  - Rise of the Privacy Shield
- **Privacy Torts**
  - Intrusion on personal seclusion
  - Public disclosure of private facts
  - False Light
  - Commercial appropriation of name or likeness

*Source:
www.injurylawsourcepa.com

Federal U.S. Cybersecurity Law and Policy

Intro to Federal U.S. Cybersecurity Policymaking

- **Goal**: Managing “cyber attacks”
- **Elements**:
  - Role of Agencies (e.g., DHS, FBI, CIA, DOD)
  - Advent of CYBERCOM
- **Evolution**:
  - Clinton Administration
  - Bush Administration
  - Obama Administration

Breakdown of U.S. Cybersecurity Legal Authorities

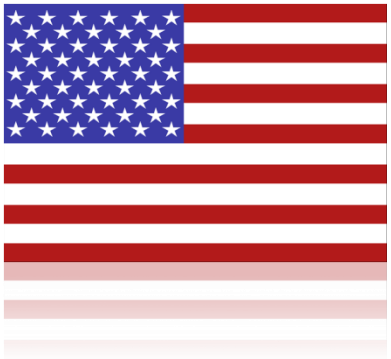
- **Anti-Hacking Laws**
  - Computer Fraud and Abuse Act (CFAA)
  - State Anti-Hacking Laws
- **Sample Private Sector Regulation**
  - Gramm-Leach-Bliley Act (GLBA) (Financial)
  - Fair & Accurate Credit Transactions Act (Red Flag Rule)
  - Fair Credit Reporting Act (FCRA) (Identity Theft)
  - Sarbanes-Oxley (SoX) (Financial)
  - Health Insurance Portability And Accountability Act (HIPPA) (Health)
  - Federal Energy Regulatory Commission (Electric Utilities)
- **Sample Public Sector Regulation**
  - Clinger-Cohen Act
  - Federal Information Security Management Act (FISMA)
  - Administrative Procedure Act (APA)

Proposed Cybersecurity Legislation

- **Early Efforts:**
  - Lieberman-Collins
  - Rockerfeller-Snowe
- **More Recent:**
  - Cybersecurity Act of 2012
  - SECURE IT Act
  - Cybersecurity Act of 2015
- **Key Sticking Point:**
  - Liability
  - Information Sharing

Global Dimension

Philosophical Differences Regarding Privacy Between US and EU



- Government use of data is restricted; private use is acceptable unless harmful or if covered by a sector-specific law (Privacy Shield)

- No one can collect or use data unless permitted to do so by law

The Global Dimension
EU Cybersecurity & Employee Data Privacy

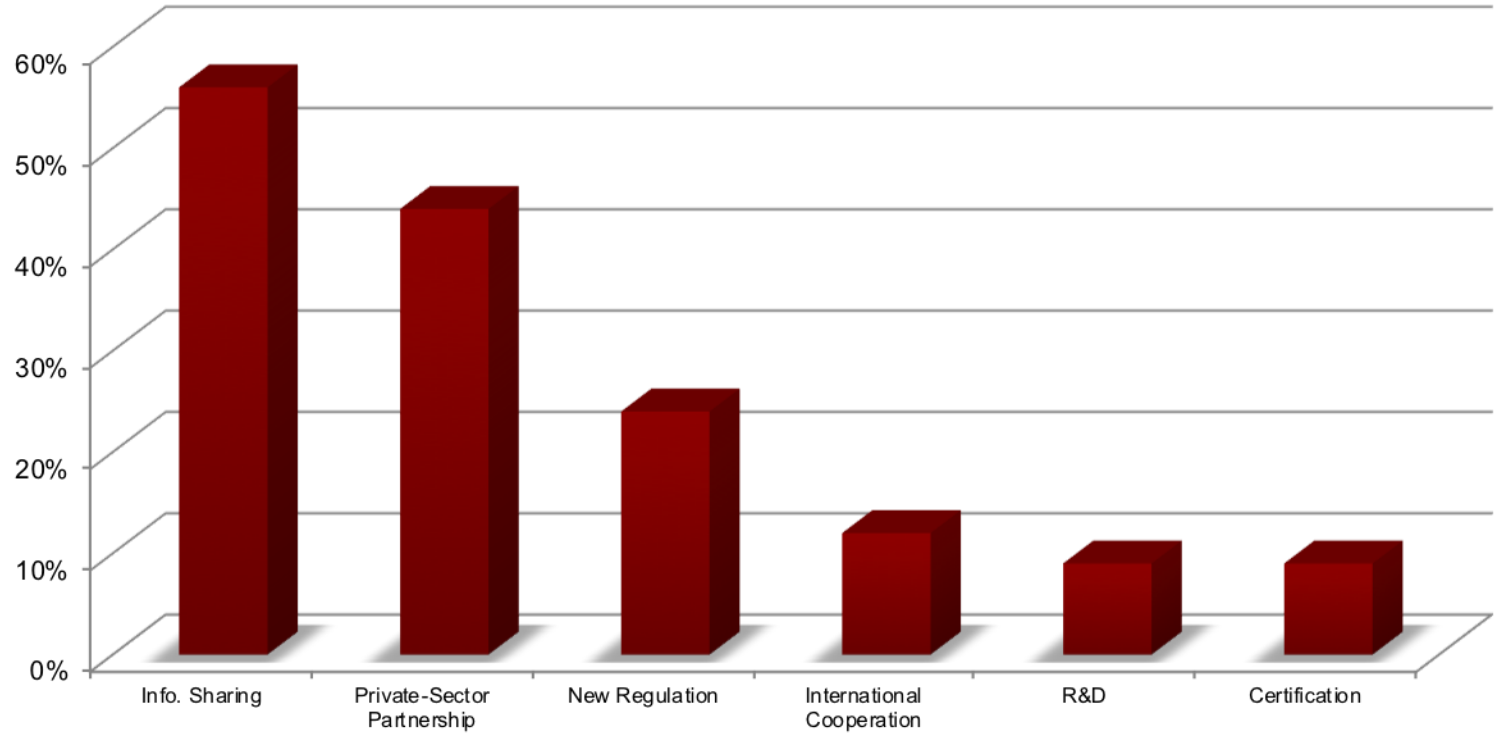
*Source: *www.euinjapan.jp*

- **National Efforts** (UK)
- **New EU Cybersecurity Strategy (Feb. 2013)**
  - Notify national authorities of “significant” cyber attacks
  - Regulate CNI as well as Internet companies
  - Impose liability even with outsourcing
- **Recent Developments**: NIS Directive & GDPR

NIST Summary Chart

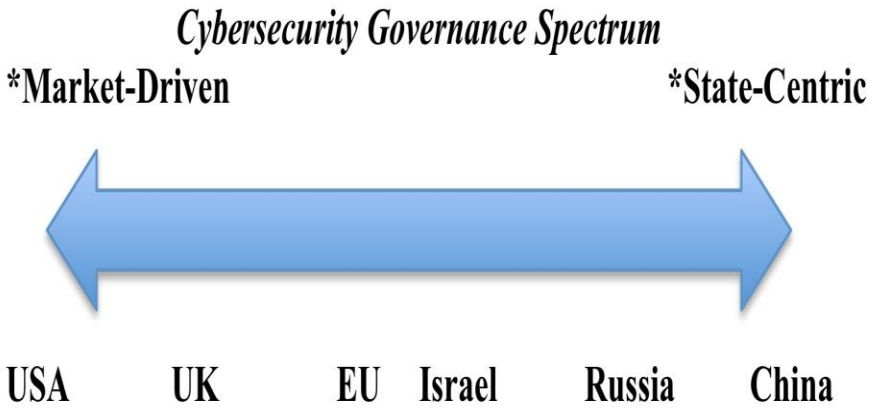
	UK	Italy	EU	Japan	South Korea	Australia
Overall NIST Framework Implementation Status	No new, updated strategy has been released since the NIST Framework was released. However, intent to harmonize NIST and UK practices has been announced formally by US and UK leaders. The recent release of 10 Steps: Advice Sheets track elements of NIST Framework.	General intention to identify international best practices announced. No specific mention of NIST harmonization or implementation, but certain language overlaps imply NIST influenced Italian cybersecurity strategies.	NIS Directive still in flux, but is close to implementation. At least one meeting was held regarding the merits of standardizing NIST and NIS Platform, and results of latest NIS Working Group meeting indicate implementation is likely.	Pending[1]	Pending[2]	Pending[3]
Overlap with NIST Framework Approach	Emphasis that implementation of framework may be variable depending on the business, and is adaptable over time. Enables internal risk management processes, implementation variable based on risk appetite.	Espouses best practices in the language of the NIST Core: analyzing, preventing, mitigating, and reacting to cyber threats.	Exact language of NIST core has been proposed for formal adoption into NIS Directive.	Emphasis on voluntary standards and public/private cooperation.	Utilizes some market-developed standards.	General emphasis on voluntary standards and public/private cooperation, and risk management.
Differences with NIST Framework Approach	Not broken down by Function, etc. Rather, collected in "Advice Sheets" intended to assist firms. Compliance is required to achieve Cyber Essentials certification.	Broken down in a pyramid structure, with risk analysis, management, and mitigation forming the base, and identifying training, awareness and "empowerment" as the capstone. Emphasis on preventing cybercrime.	Less focus on responding to cyber threats, and does not emphasize public relations and reputational damage caused by incidents. Steps for detecting and protecting against intrusions sometimes overlap.	(Unavailable at this time.) Potentially a greater reliance on government incentives than risk management.	Mandatory. Standards primarily government developed. More top-down than NIST Framework.	(Unavailable at this time.) Potentially a greater reliance on private/private partnerships.

Critical Infrastructure Dimension Summary Chart



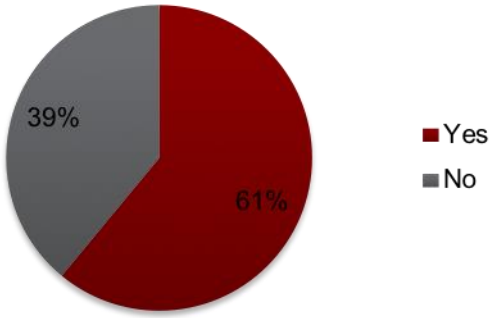
Regulating Cyberspace

- Governance Spectrum

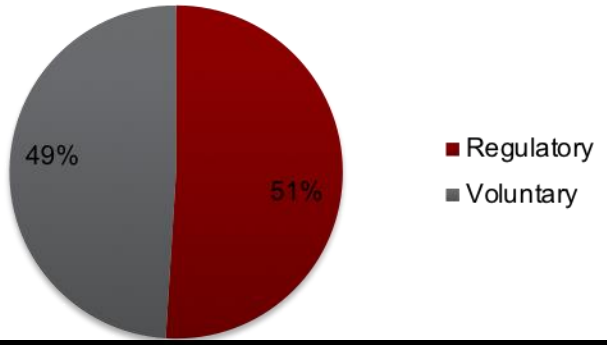


- Voluntary vs. Regulatory Approach

Suffered Cyber Attack in Past 12 Months?

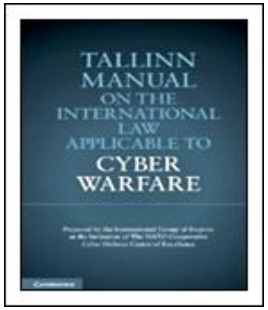


Approach Favored in Managing Cyber Attacks?



Role of International Law

- **Camps**
  - IL should apply
  - New treaty
  - No hope
  - Some hope, but *state-centric*



*Source: *CCDCOE*

**Source*: *ITU*

- **Toward a Law of Cyber Peace?**
  - **Countermeasures**
  - **State Responses**
  - **Analogies**
    - Nuclear War
    - Outer Space
    - Antarctica
  - **Other Applicable Accords**
    - Mutual Legal Assistance Treaties
    - Vienna Convention on Diplomatic Relations
    - *Bilateral Investment Treaties*
- ***Summary**: It's a patchwork, but it's a beginning!*

Global Cybersecurity Governance Sim

Background: *As Richard Clarke discussed in his op-ed, multilateral Internet governance is difficult. But getting a handle on problems ranging from cyber war to crime, terrorism, and espionage requires nations to work together and find common ground. Discuss in groups the following issues and see where you come down.*

Discuss:

1: What are some of the benefits and drawbacks of the "like-minded" approach to negotiations for which Clarke argues?

2: Is it possible (or desirable) to ban cyber weapons?

3: What role (if any) should international institutions, like the International Telecommunication Union, have in cybersecurity?

Attribution Dilemmas

Technical Problems

- Science of tracing cyber attacks is still developing
- Web architecture
- Cyber defense alone is not enough

*Source: DoD Images

Legal Problems

- Underdeveloped legal regimes
- Applicable treaties lack enforcement mechanisms
- Attribution and state responsibility

*Source: Hacker News

Defining "Cyber Peace"

Vatican's Pontifical Academy of Sciences Erice Declaration on Principles for Cyber Stability and Cyber Peace

1. All governments should recognize that **international law guarantees individuals the free flow of information and ideas**; these guarantees also apply to cyberspace. Restrictions should only be as necessary and accompanied by a process for legal review.
2. All countries should work together to **develop a common code of cyber conduct and harmonized global legal framework**, including procedural provisions regarding investigative assistance and cooperation that respects privacy and human rights. All governments, service providers, and users should support international law enforcement efforts against cyber criminals.
3. All users, service providers, and governments should work to ensure that **cyberspace is not used in any way that would result in the exploitation of users**, particularly the young and defenseless, through violence or degradation.
4. Governments, organizations, and the private sector, including individuals, should implement and maintain **comprehensive security programs based upon internationally accepted best practices** and standards and utilizing privacy and security technologies.
5. Software and hardware developers should strive to develop **secure technologies that promote resiliency** and resist vulnerabilities.
6. Governments should actively participate in **United Nations' efforts to promote global cyber security and cyber peace** and to avoid the use of cyberspace for conflict.

Summary & Take Aways

Next Steps

- Proactively invest in enhancing cybersecurity
- Assess current insurance coverage and ERM plan
- Seek out partnerships to share threat information

State Governments

- ISACs/ISAOs
- Clinical collaboration
- Bug bounty programs
- Cybersecurity awareness raising activities
- Training programs
- Data breach notification
- NIST Framework compliance

Thank you!
Questions?

Contact Info: sjshacke@indiana.edu

Further Reading:

1) *Should Your Firm Invest in Cyber Risk Insurance?*, 55 BUSINESS HORIZONS 349 (July-Aug. 2012)
2) *Risky Business: Lessons for Mitigating Cyber Attacks from the International Insurance Law on Piracy*, 24 MINNESOTA JOURNAL OF INTERNATIONAL LAW ONLINE 33 (2015) (with Scott Russell)
3) *Cyber Insurance: A Last Line of Defense When Technology Fails*, LATHAN & WATKINS (2014)