Securing the Internet of Things & State of Hoosier Cybersecurity

Prof. Scott Shackelford JD, PhD

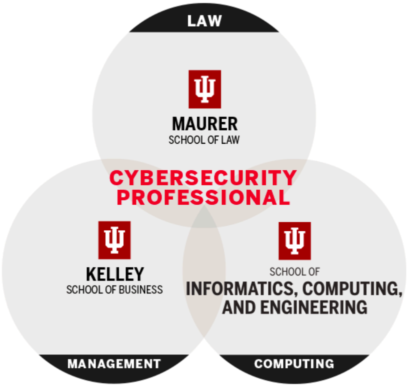
KELLEY SCHOOL OF BUSINESS

INDIANA UNIVERSITY

INDIANA UNIVERSITY

IU Cybersecurity Risk Management

- Multidisciplinary Program (Law, Secure Computing, & Business)
- Built on IU's Cybersecurity Certificates
- Applied Cybersecurity Risk Management Capstone
- Online courses available
- Size: 100+ (Spring 2020)
- Advisory Council

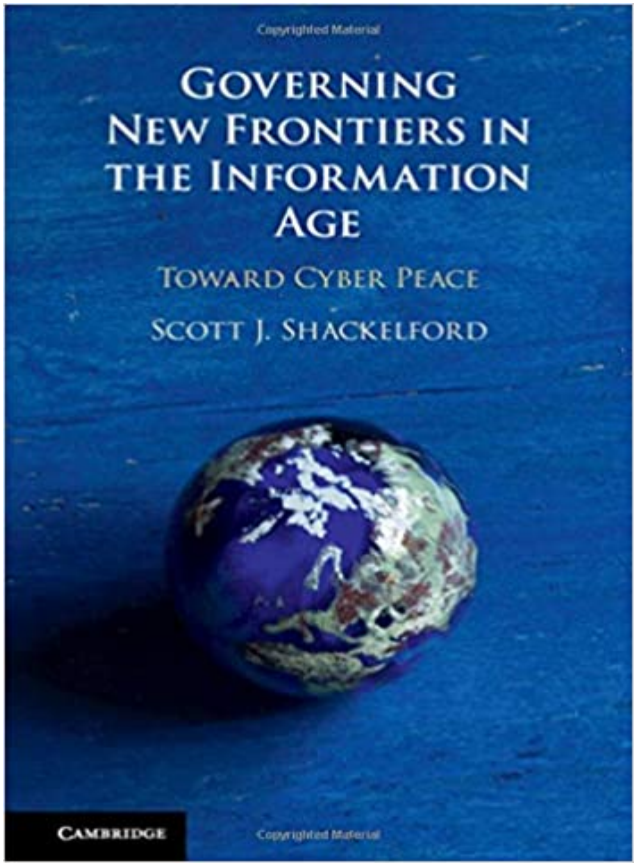


Ostrom Workshop Program on Cybersecurity & Internet Governance

- ***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

Recent Research



Copyrighted Material

GOVERNING NEW FRONTIERS IN THE INFORMATION AGE

TOWARD CYBER PEACE

SCOTT J. SHACKELFORD

CAMBRIDGE

Copyrighted Material

THE INTERNET OF THINGS

WHAT EVERYONE NEEDS TO KNOW®

SCOTT J. SHACKELFORD

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

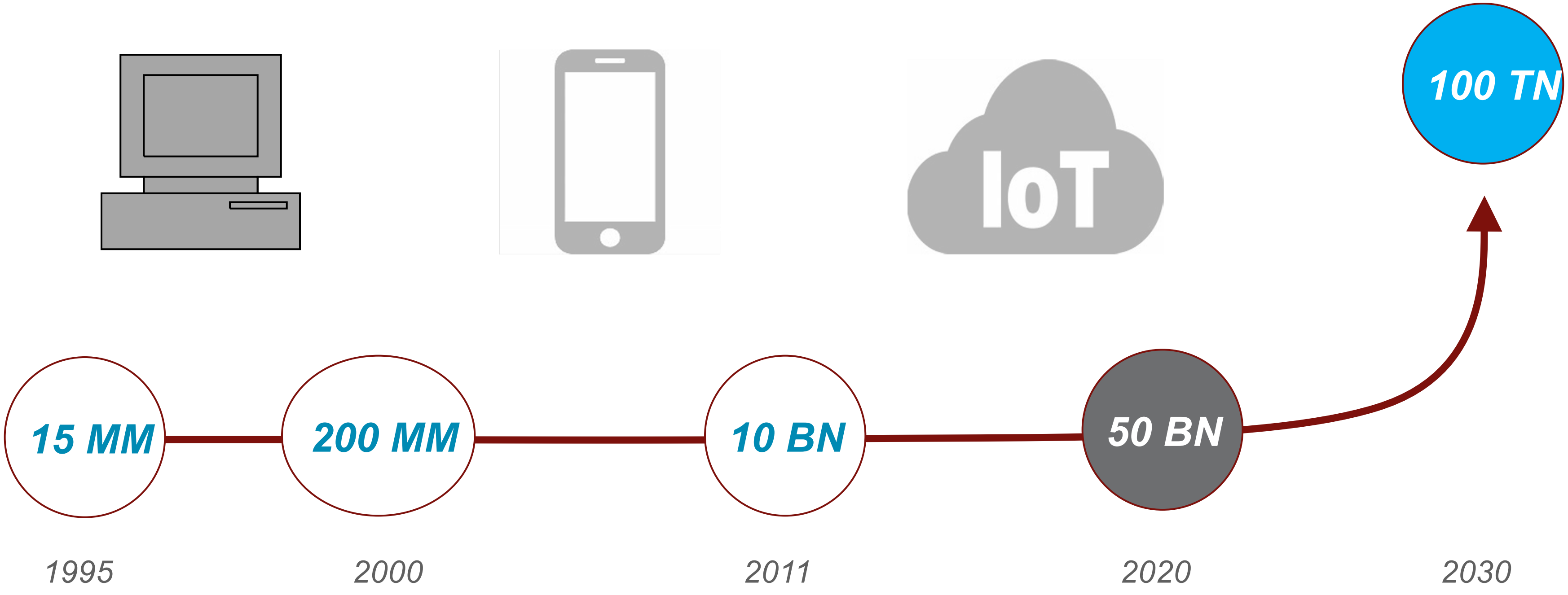
- Fear of "Electronic Pearl Harbor" (overblown?)
- Protecting critical national infrastructure

Q: WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE.. BACK HERE
CYBER SECURITY

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



15 MM
1995

200 MM
2000

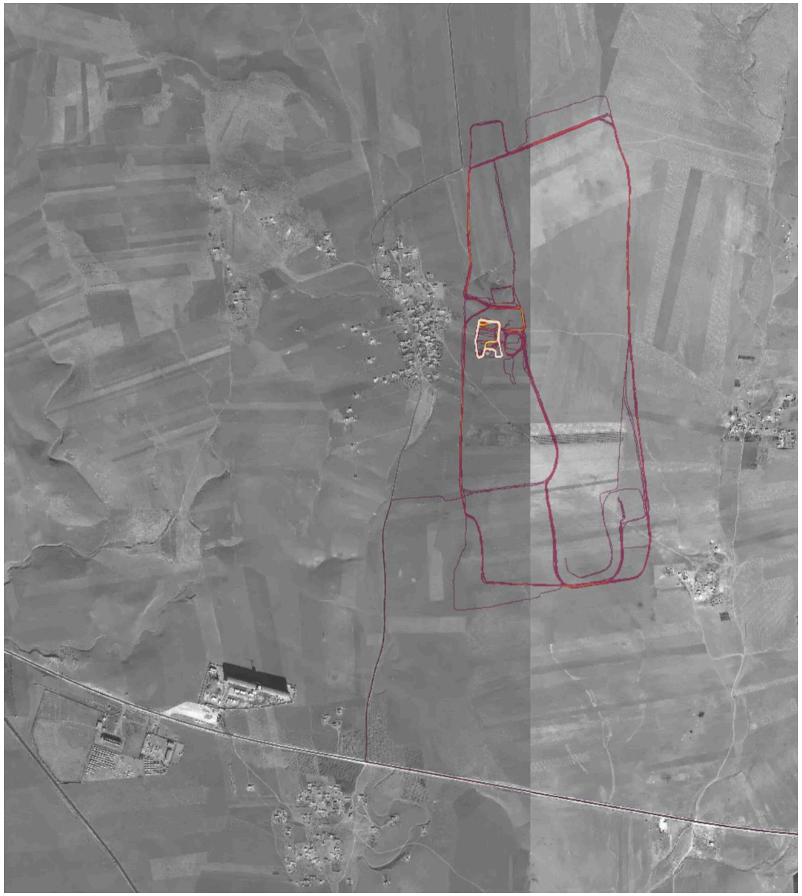
10 BN
2011

50 BN
2020

100 TN
2030

Source: Oliver Wyman analysis

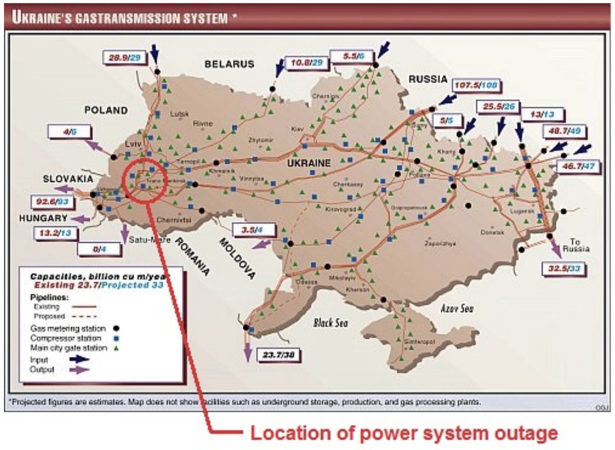
Example: Strava GPA Global ‘Heatmap’



**Source: Fortune*

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)

So What Do We Do About It? Introducing the Three Dimensions of Cybersecurity Risk Management

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

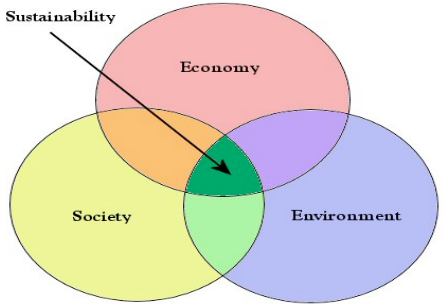
Former Director of National Intelligence James R. Clapper
Worldwide Cyber Threats Testimony, Sep. 10, 2015

Throwing Money at the Problem

- **U.S. Private Sector Spending on Cybersecurity** - $102 billion by 2020 (a 38% increase from 2016)
- **U.S. Public Sector Spending on Cybersecurity** - $28 billion in 2016 (compared to $7.5 billion in 2007)
- **How much is too much?** According to the Gordon-Loeb theory, the optimal amount is *37% of the projected loss*.

Investigating Analogies: Cybersecurity as Social Responsibility

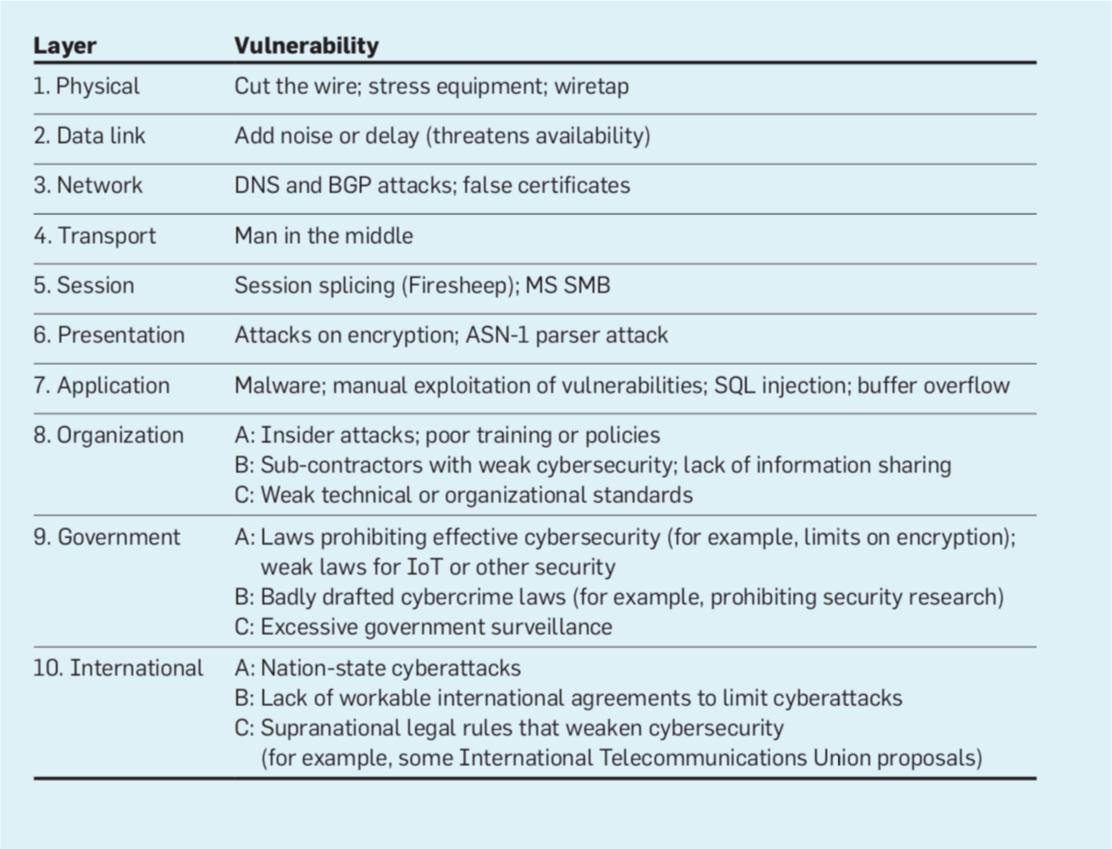
- **Problems**: Is there a tragedy of the cyber commons? Putting it another way, is there a market failure here? Where does cost-benefit analysis fall short?
- **Idea**: Measure impact of a firm's operation on the broader Internet ecosystem.
- **Some Applicable Tools**:
  - Integrated Reporting
  - Certificate Programs
  - Environmental Law Analogies
- **Drawbacks**?



*Source: *www.keepoklahomabeautiful.com*

What does it mean to manage cyber attacks from the bottom-up?

Introducing the Cybersecurity Stack (Swire 2018)



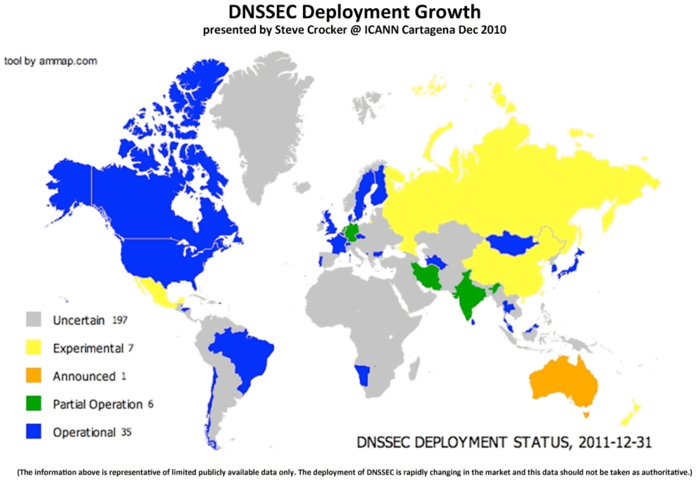
Layer	Vulnerability
1. Physical	Cut the wire; stress equipment; wiretap
2. Data link	Add noise or delay (threatens availability)
3. Network	DNS and BGP attacks; false certificates
4. Transport	Man in the middle
5. Session	Session splicing (Firesheep); MS SMB
6. Presentation	Attacks on encryption; ASN-1 parser attack
7. Application	Malware; manual exploitation of vulnerabilities; SQL injection; buffer overflow
8. Organization	A: Insider attacks; poor training or policies B: Sub-contractors with weak cybersecurity; lack of information sharing C: Weak technical or organizational standards
9. Government	A: Laws prohibiting effective cybersecurity (for example, limits on encryption); weak laws for IoT or other security B: Badly drafted cybercrime laws (for example, prohibiting security research) C: Excessive government surveillance
10. International	A: Nation-state cyberattacks B: Lack of workable international agreements to limit cyberattacks C: Supranational legal rules that weaken cybersecurity (for example, some International Telecommunications Union proposals)

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


DNSSEC Deployment Growth
presented by Steve Crocker @ ICANN Cartagena Dec 2010
tool by ammap.com
Uncertain 197
Experimental 7
Announced 1
Partial Operation 6
Operational 35
DNSSEC DEPLOYMENT STATUS, 2011-12-31
(The information above is representative of limited publicly available data only. The deployment of DNSSEC is rapidly changing in the market and this data should not be taken as authoritative.)

*Source: www.techbyte.pl

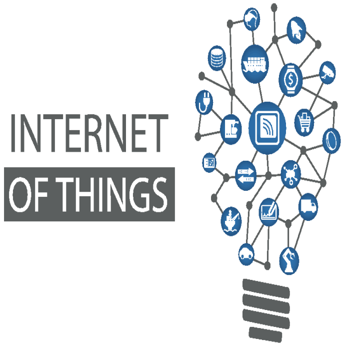
Private-Sector Cybersecurity Best Practices

- **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

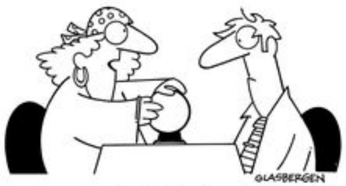
*Source: www.wizilegal.com

Fixing an Internet of Broken Things

1. Deeper cooperation both within and between IoT sectors
2. Develop standards for IoT devices using the NIST CSF and CPS as guides
3. Promote flexible, guidance-driven frameworks to promote resilience, including in supply chains
4. Use government contracting as a mechanism to promote cybersecurity due diligence
5. Boost FTC and SEC resources to go after bad actors and enforce reporting requirements



"I'm From the Government and am Here to Secure Your Device"



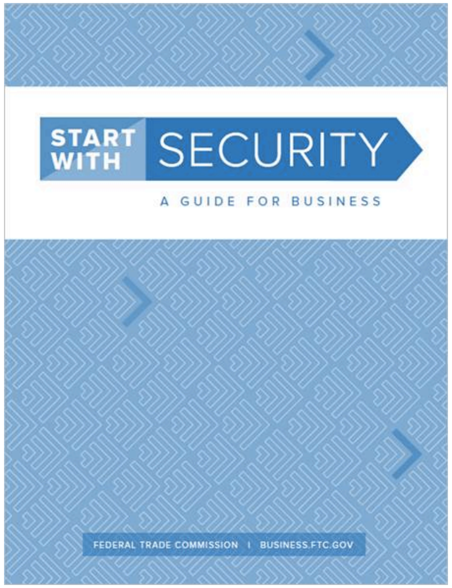
© Randy Glasbergen
glasbergen.com

"I can't see your future, but I found your bank files, Social Security number and all of your company passwords."

- **U.S. Federal Efforts**
  - – Federal Trade Commission
  - – NIST Cybersecurity Framework & IOT
  - – Unpacking the Proposed IoT Cybersecurity Improvement Act of 2019
  - – Graves Bill
- **State-Level Efforts**
  - – California 2018 Consumer Privacy & IoT Acts
- **Civil Society**
  - – Consumer Reports Digital Standard

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



START WITH SECURITY

A GUIDE FOR BUSINESS

FEDERAL TRADE COMMISSION | BUSINESS.FTC.GOV

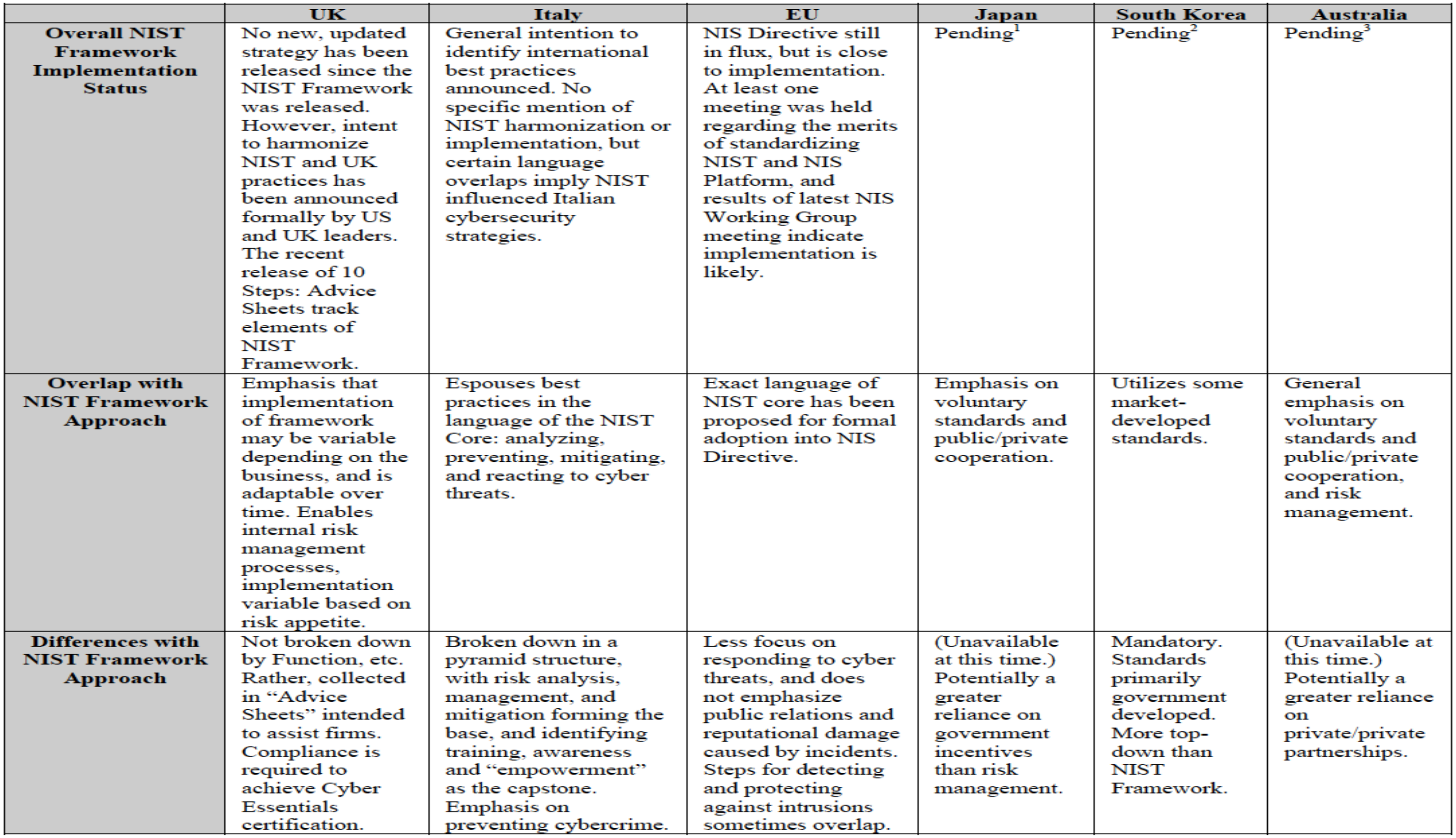
Negligence and the NIST Cybersecurity Framework

- **2013 State of the Union Address**
  - Focus on cyber threats to nation's critical infrastructure

*Source: *welivesecurity.com*

- **Executive Order 13636: Improving Critical Infrastructure Cybersecurity**
  - Increase information sharing
  - Ensure privacy and civil liberties protections
  - Develop a voluntary Cybersecurity Framework

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.

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

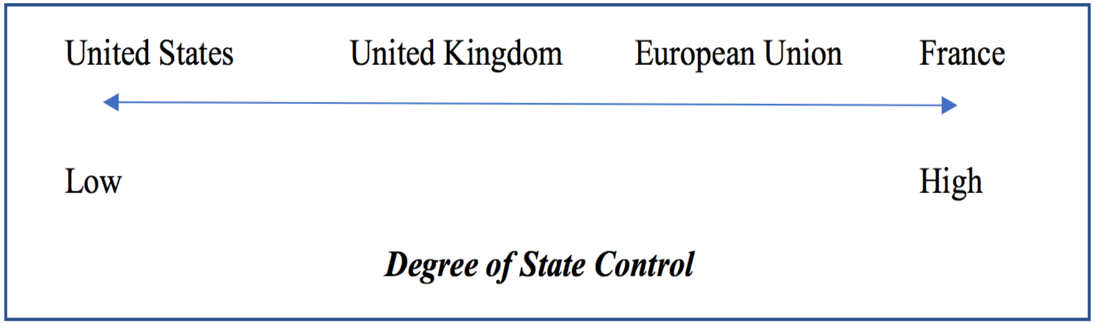
**Source: IAPP*

Approaches to IoT Governance

Type of Approach	Description	Example Jurisdiction
Safe Harbor	Incentivizing businesses to “develop and maintain a cybersecurity program that ‘reasonably conforms” to an already existing, industry-recognized cybersecurity framework” like the NIST CSF.	Ohio
Reasonableness Standard	“Any manufacturer of a device that connects “directly or indirectly” to the Internet must equip it with “reasonable” security features, designed to “prevent unauthorized access, modification, or information disclosure.”	California
Dislosure Requirements	“Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and. incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.”	SEC; state-level
Data Privacy & Codes of Conduct	Incentivizes firms to develop industry codes of conduct to consider the wider risk of cyber threats to IoT ecosystems.	GDPR
IoT Trustmarks	Focusing on consumers by informing them of the risks posed by various IoT devices and services.	EU CE Marking
Products Liability	Treating breaches related to IoT products under a strict liability standard.	France

Regulating IoT Globally

- Governance Spectrum



United States

United Kingdom

European Union

France

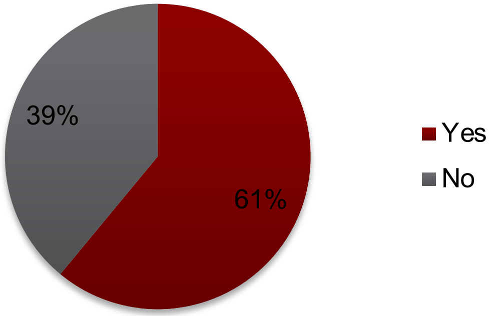
Low

High

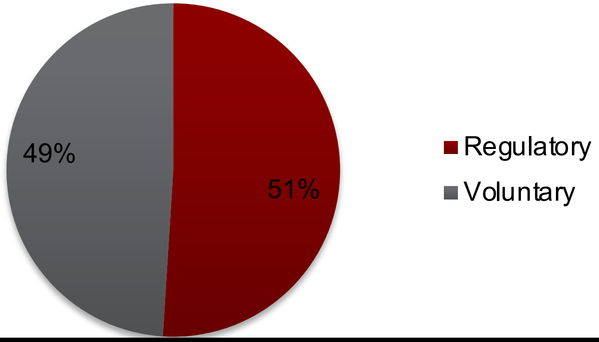
Degree of State Control

- "Voluntary" vs. "Regulatory" Approaches

Suffered Cyber Attack in Past 12 Months?



Approach Favored in Managing Cyber Attacks?



Regime Effectiveness of IoT Governance through the Lens of the Ostrom Design Principles

Ostrom Design Principle	Applicability	Example Regulatory Regime	Explanation
Clearly Defined Boundaries	Contested	NIST CSF; FTC Guidelines	Defined boundaries are problematic given the extent to which various smart devices from automobiles to thermostats, and even toasters, interconnect to form ecosystems.
Fit to Local Conditions & Proportionality	Fostered	UK Cyber Essentials Plus Certificate; Digital Standard; Internet of Things Cybersecurity Act of 2017 (proposed)	The problem of proportilinaty is a frequent refrain in the cybersecurity context where few providers invest as much as they should in proactive cybersecurity measures because the full benefits of such investments are not realized by the firm.
Collective-Choice Arrangements	Fostered	NIST CSF; Paris Call	This principle implies the importance of engaged and proactive rulemaking by technical communities, the private sector, and the international community.
Monitoring	Fostered	Digital Standard; FTC; European Commission; Cybersecurity Tech Accord	According to Professor Ostrom, trust can typically only do so much to mitigate rule-breaking behavior. Eventually, some level of monitoring becomes important. In self-organized communities, typically monitors are chosen among the members to ensure “the conformance of others to local rules.”
Graduated Sanctions	Fostered	GDPR; 2018 California Law; FTC	Rule violations must not pass without notice or correction by the group.
Minimal Recognition of Rights to Organize	Present	GDPR, U.S. Constitution	This principle recognizes the importance of permitting stakeholders a say in organizing collective rules.
Nested Enterprises	Present	IETF; Consumer Reports; Information Sharing and Analysis Centers (ISACs)	Underscores the extent to which multilevel, multi-stakeholder governance structures are vital to instill governance best practices.

Teaching IoT Security : IU Cybersecurity Clinic

- **Goals**
- **Past Projects**
  - – State Government/INoT
  - – Speedway, IN
  - – MCCSC
  - – Microsoft
  - – Consumer Reports
  - – Election Security
- **Future Plans**

State-Level Snapshot: Indiana

State of Hoosier Cybersecurity

2020

December 2020

Prepared for
Indiana Executive Council on Cybersecurity
By
Kelley School of Business, Indiana University
Indiana Business Research Center
Anne Boustead JD, PhD (University of Arizona), Scott Shackelford JD, PhD (Indiana University)

Special thanks to Jay Bhatia and Eric Spencer for their invaluable research support in this project. We would also like to thank the anonymous respondents who participated in our survey on behalf of their organizations, and to Stephen Vina, and Professors Asaf Lubin and Angie Raymond for their helpful comments and suggestions.

CYBERSECURITY PROGRAM

OSTROM WORKSHOP

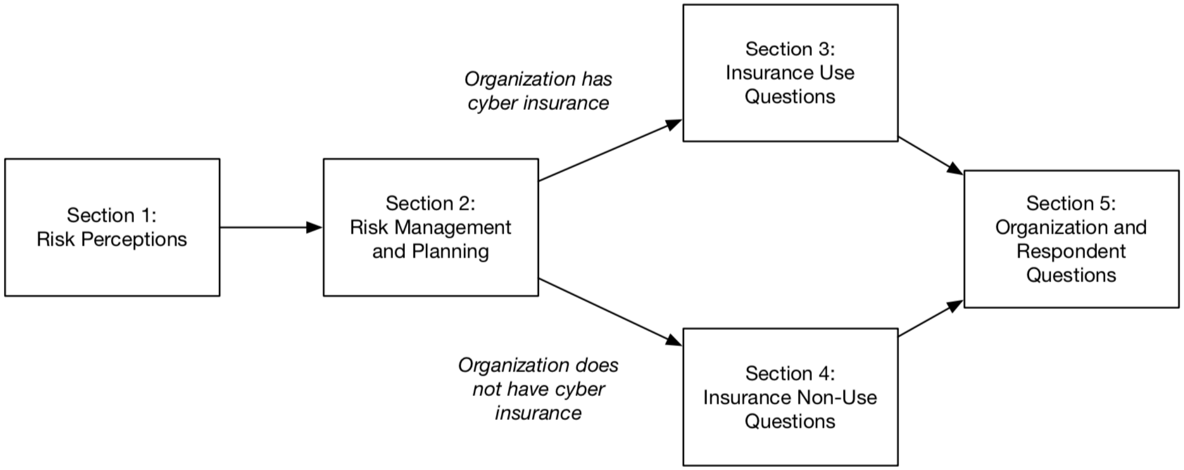
IBRC

Motivation

- Ensuring businesses and government entities engage in strong cybersecurity practices is important for protecting economic and security interests
- However, there is still much to learn about whether, how, and why organizations decide to engage in cybersecurity practices
- Decided to investigate this question in the context of Indiana

Methodology

Cybersecurity Survey Flow Logic



Section 1:
Risk Perceptions

Section 2:
Risk Management
and Planning

Organization has cyber insurance

Organization does not have cyber insurance

Section 3:
Insurance Use
Questions

Section 4:
Insurance Non-Use
Questions

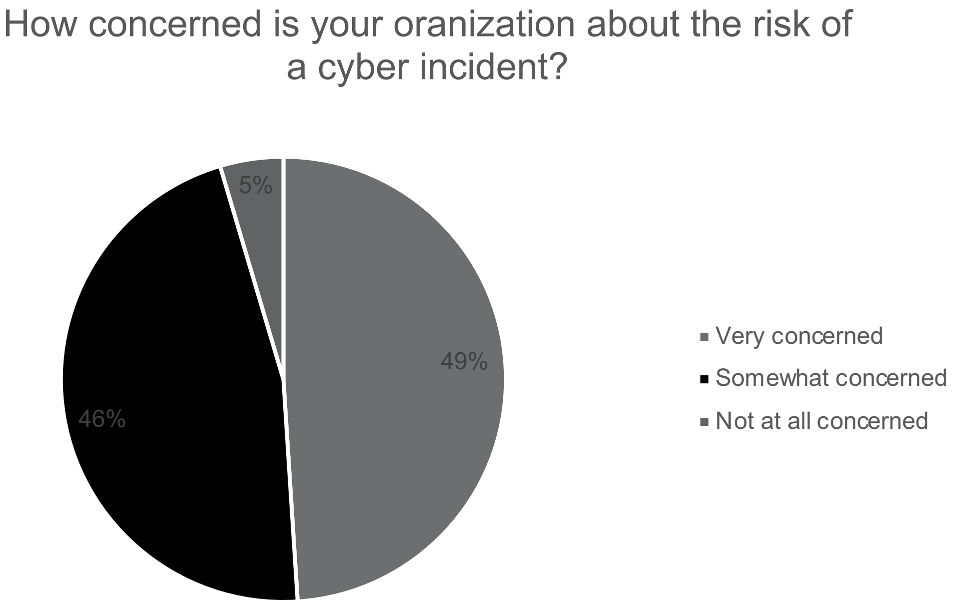
Section 5:
Organization and
Respondent
Questions

Important Caveats

- We are still in the process of analyzing the results of the survey

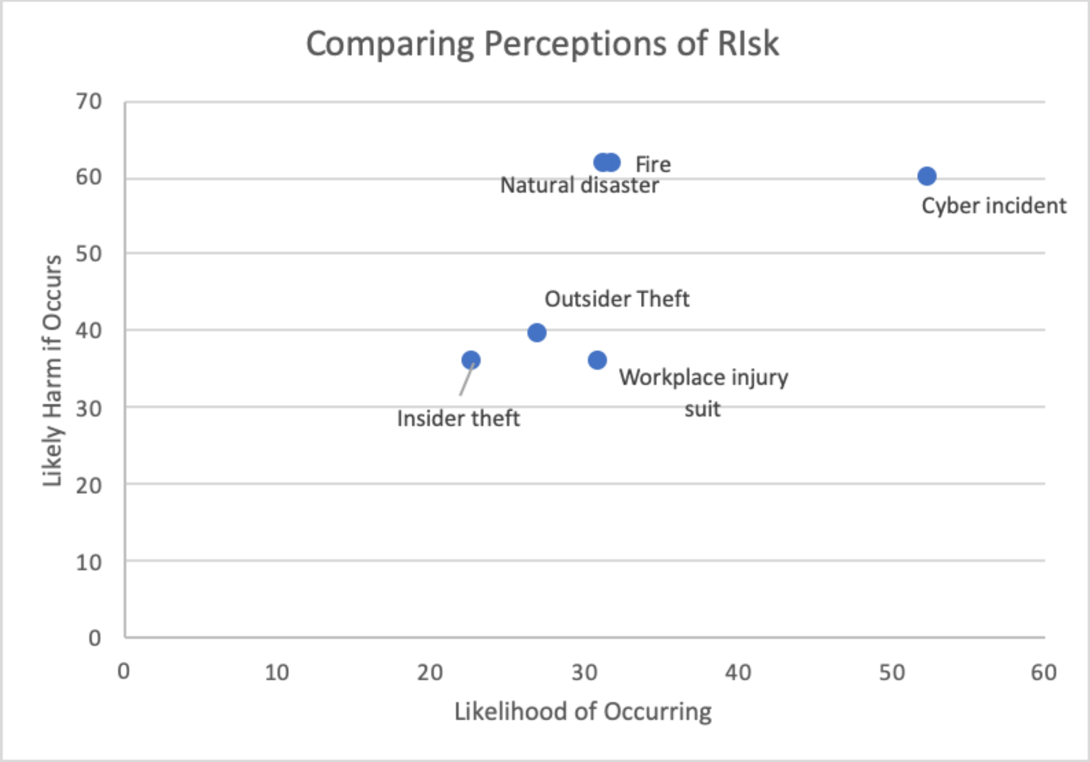
- Results presented today are early preliminary results, and are subject to change

Indiana organizations are generally concerned about the risk of a cyber incident

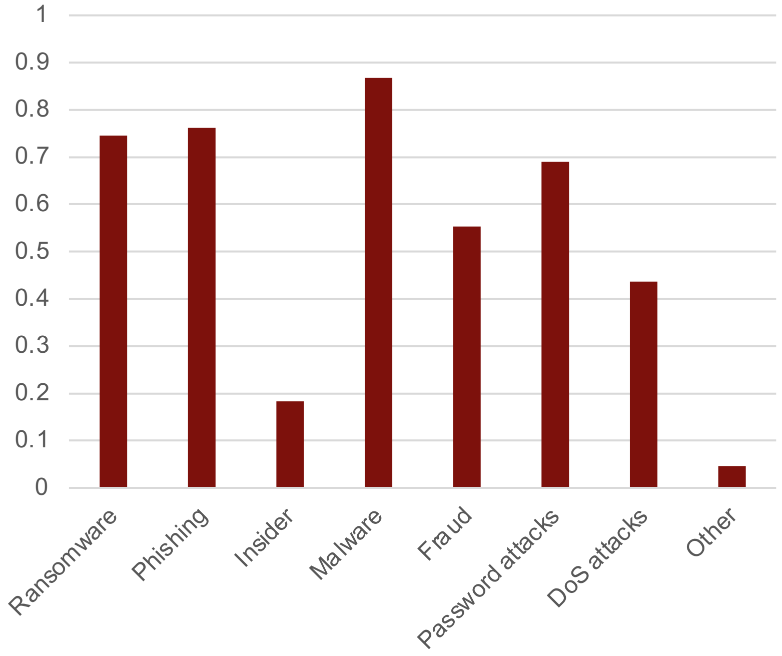


- Levels of concern are high amongst both critical infrastructure organizations and non-critical infrastructure organizations

Cyber incidents are perceived as more severe than other types of potential harms

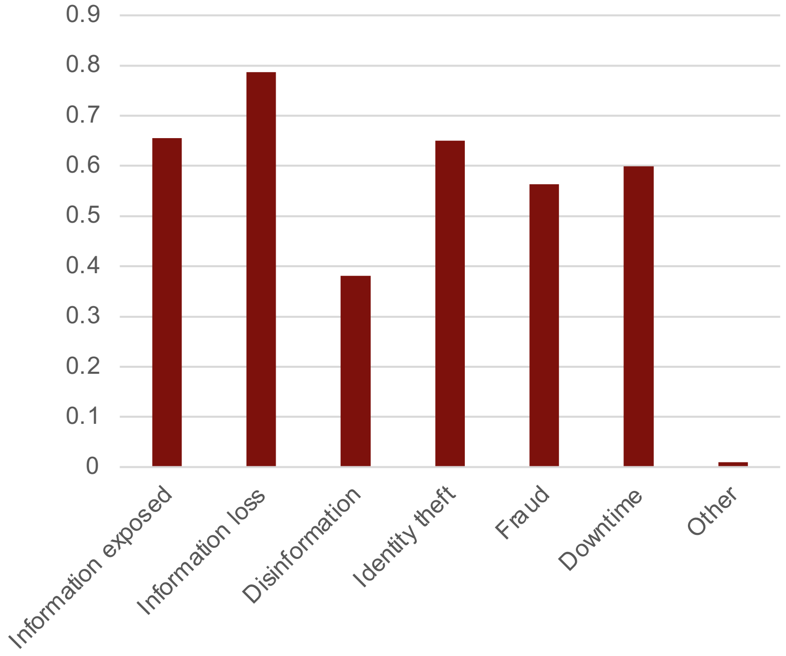


What types of cyber incidents are Indiana organizations concerned about?



- Respondents were also asked to rank which they were most concerned about. Allocating more points for a higher ranking yields this ranking:
  - Ransomware
  - Phishing
  - Malware
  - Fraud
  - Password
  - Denial of service attack
  - Insider attack
  - Other

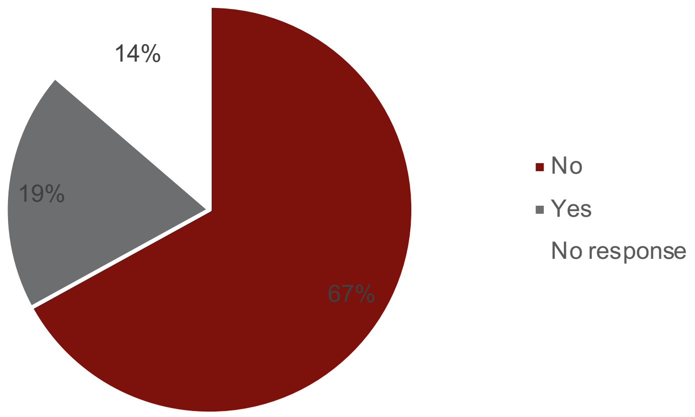
What consequences of cyber incidents are Indiana organizations concerned about?



- Respondents were also asked to rank which they were most concerned about. Allocating more points for a higher ranking yields this ranking:
  - Data loss
  - Data exposure
  - Identity theft
  - Fraud
  - Downtime
  - Disinformation
  - Other

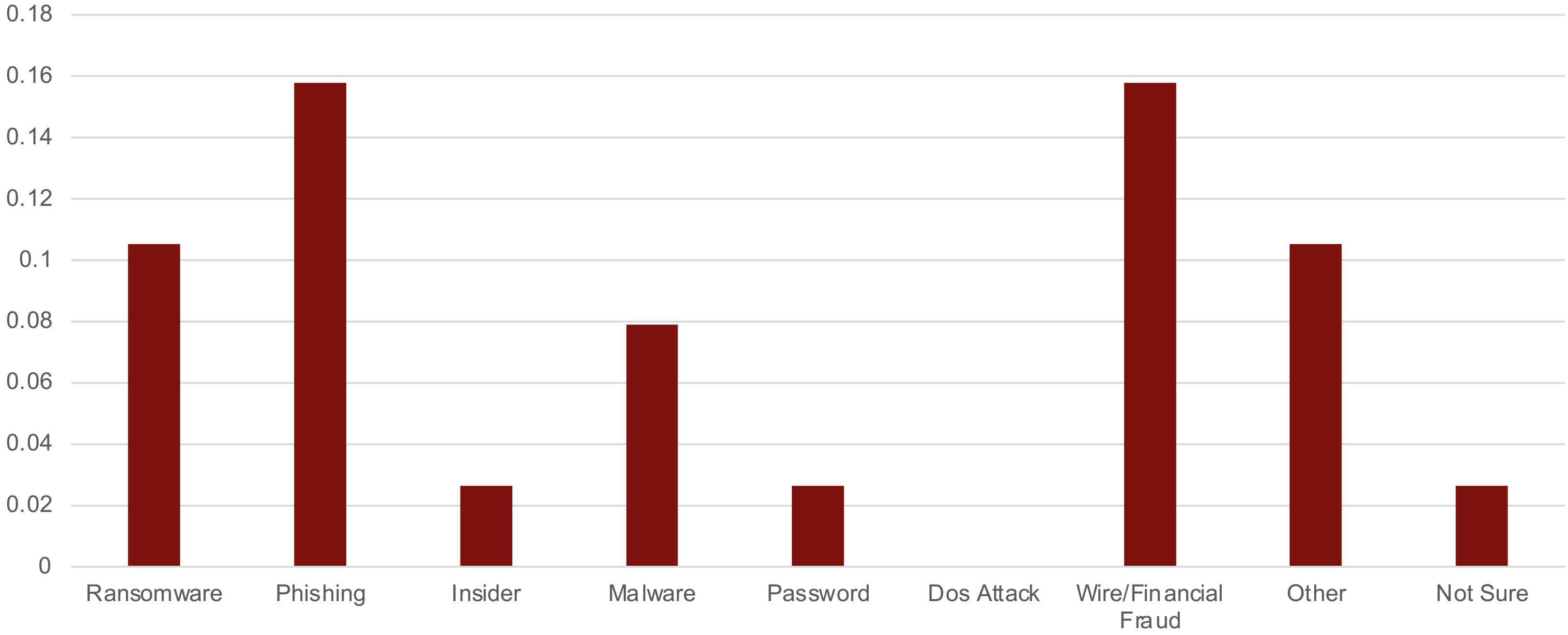
Most organizations surveyed had not experienced a cyber attack in the past three years

To your knowledge, has your organization experienced a successful cyber incident in the past three years?

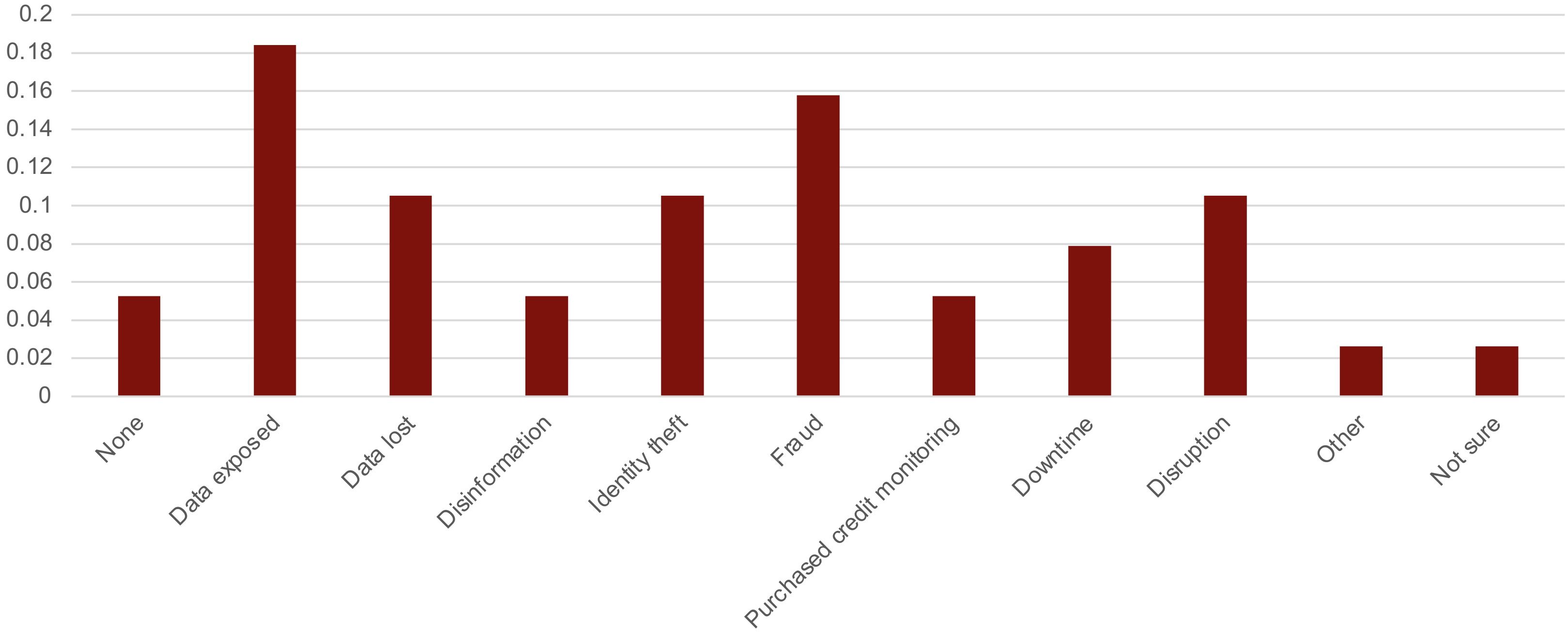


- Fewer organizations in critical infrastructure sectors reported successful cyber attacks than non-critical infrastructure organizations
  - About 13% of critical infrastructure organizations reported successful attacks
  - About 28% of non-critical infrastructure organizations reported successful attacks

Type of Attacks Experienced



Consequences of Attacks Reported

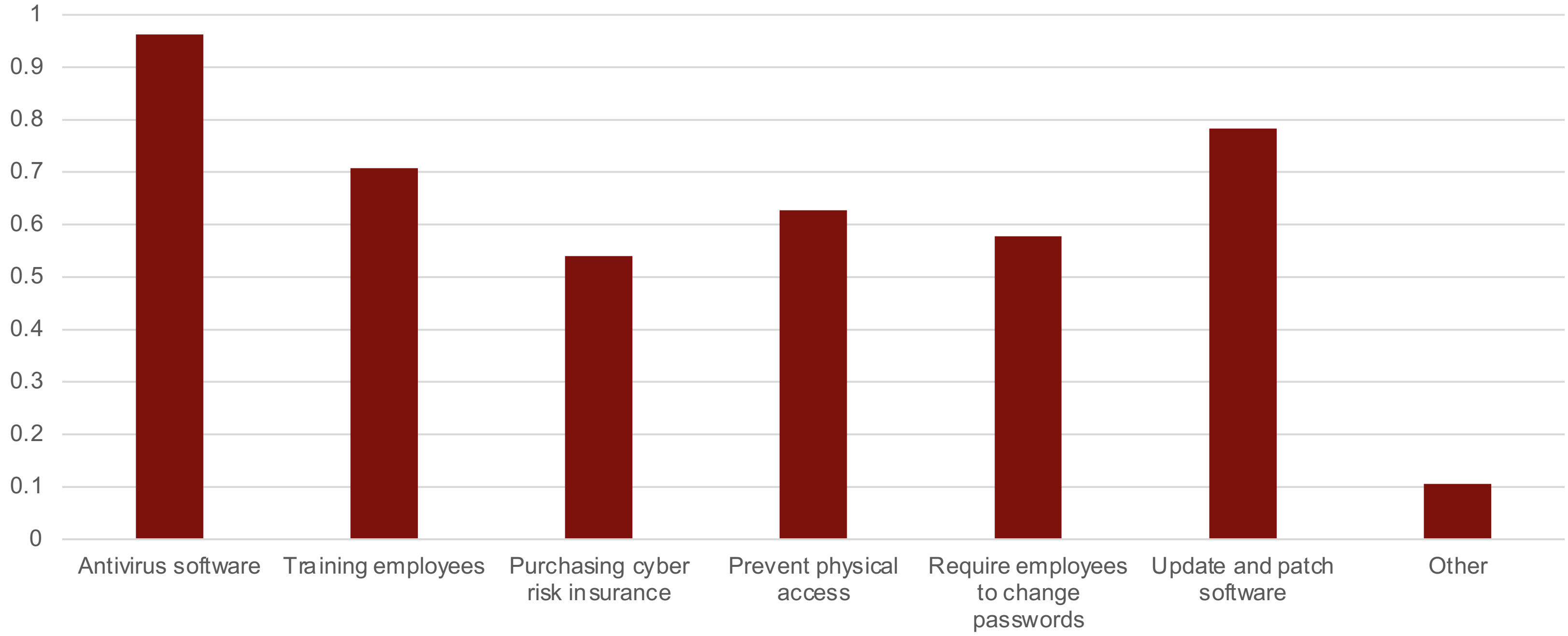


Most Indiana organizations report taking steps to prevent cyber incidents

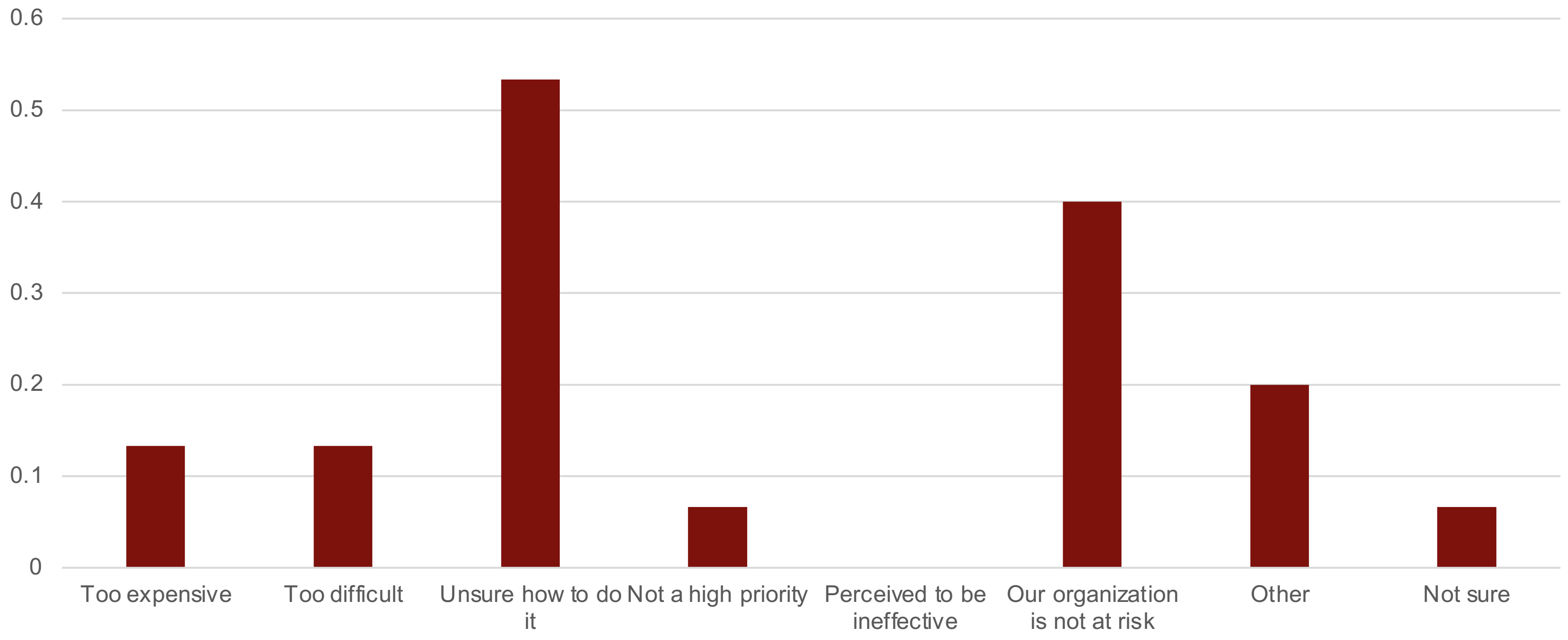
- Just over 91% of organizations surveyed said they had taken some steps to prevent cyber incidents

- Slightly more critical infrastructure organizations said they had taken steps to prevent cyber incidents, when compared to non-critical infrastructure organizations
  - About 94% of critical infrastructure organizations reported taking cyber incident prevention steps
  - About 88% of non-critical infrastructure organizations reported taking cyber incident preventions steps

Steps Taken to Prevent Cyber Incidents



Reasons why organizations did not take preventative steps



Questions?

sjshacke@indiana.edu