Identifying How Firms Manage Cybersecurity Investment

Tyler Moore

Security Economics Laboratory
Tandy School of Computer Science
The University of Tulsa

Based on joint work with Scott Dynes and Frederick Chang, SMU

Workshop on the Economics of Information Security
University of California, Berkeley
June 13, 2016

How do firms manage cybersecurity investment?

- Level of attention paid to cybersecurity by firms has skyrocketed
- But how do these firms manage cybersecurity risks?
  - Do they follow risk management guidelines?
  - Are quantitative metrics used to guide investment decisions?
  - Are the market failures actually a barrier to investment?
- In 2015, we interviewed 40 chief information security officers (CISOs) and other executives from large organizations to better understand how decisions are made in "the real world"

THE UNIVERSITY of TULSA

Outline

1. Methodology
   - Semi-structured interviews
2. Findings
   - Organizational support for cybersecurity
   - How are cybersecurity investment decisions made?
   - Is security still a market for lemons?
   - Special challenges for government CISOs

THE UNIVERSITY of TULSA

Outline

1. Methodology
   - Semi-structured interviews
2. Findings
   - Organizational support for cybersecurity
   - How are cybersecurity investment decisions made?
   - Is security still a market for lemons?
   - Special challenges for government CISOs

Semi-structured interviews

- Population of 40 CISOs, CIOs and related executives
  - Mostly large companies from healthcare (5), retail (8), finance (8) or government (11) sectors
  - 31 US participants, 9 non-US
  - Majority of participants identified by IBM (study sponsor), who passed contact details to us

Semi-structured interviews

- Population of 40 CISOs, CIOs and related executives
  - Mostly large companies from healthcare (5), retail (8), finance (8) or government (11) sectors
  - 31 US participants, 9 non-US
  - Majority of participants identified by IBM (study sponsor), who passed contact details to us
- Semi-structured interview process
  - In person or phone interviews, lasting 30 minutes to 1 hour
  - Participants were assured that their comments would be reported without attribution and not shared with IBM
  - Enabled us to build trust with subjects, glean context for responses, and gain deeper understanding of subjective approaches
  - Contextual findings do not generalize to the wider profession

THE UNIVERSITY of TULSA

Outline

1. Methodology
   - Semi-structured interviews
2. Findings
   - Organizational support for cybersecurity
   - How are cybersecurity investment decisions made?
   - Is security still a market for lemons?
   - Special challenges for government CISOs

Organizational support for cybersecurity

- Support from upper-level management
  - 81% said upper-level management are supportive or very supportive of cybersecurity efforts
  - 85% said that the level of support has been increasing
  - "Senior management has gotten religion about how important security is"

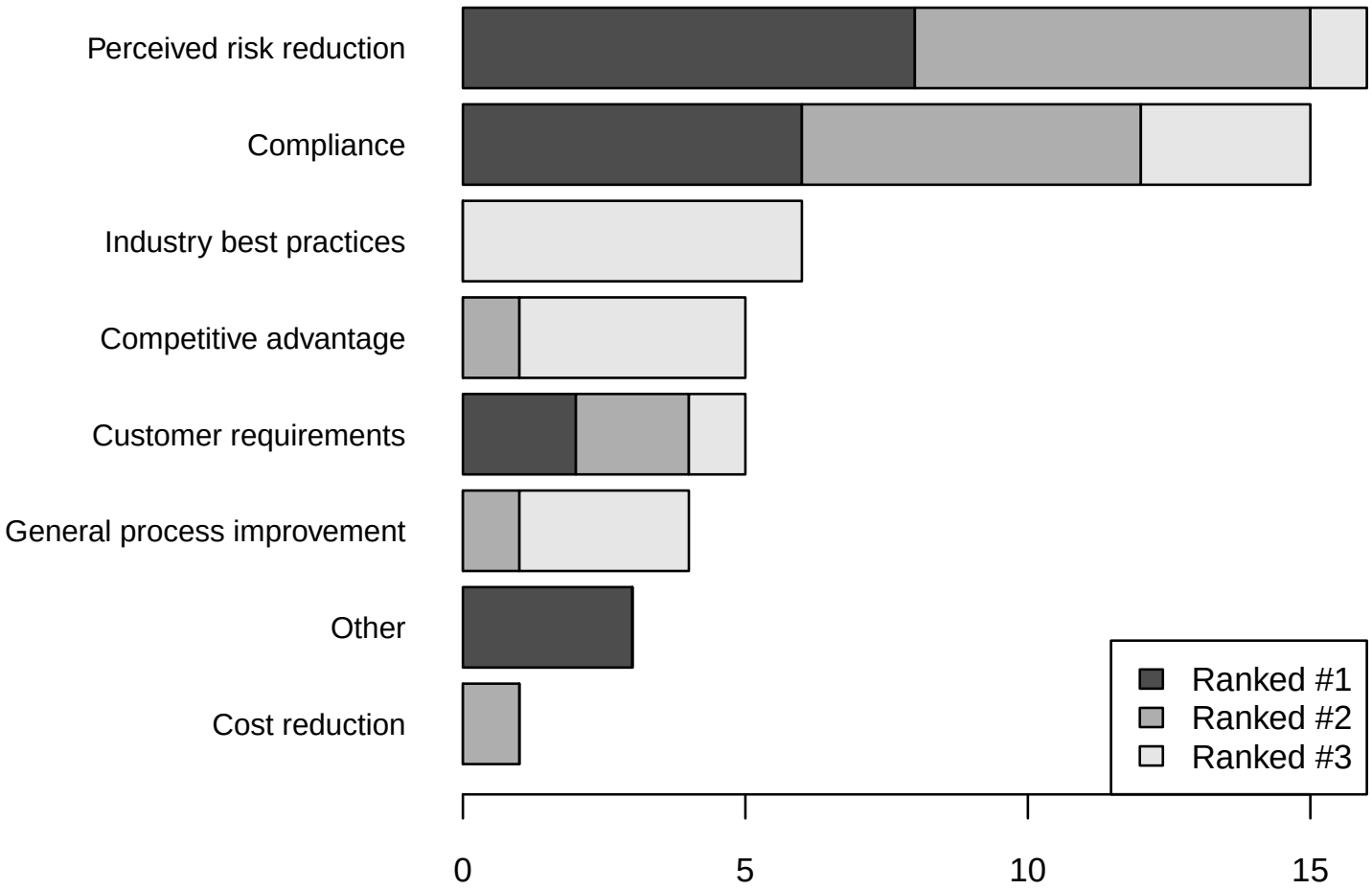
Organizational support for cybersecurity

- Support from upper-level management
  - 81% said upper-level management are supportive or very supportive of cybersecurity efforts
  - 85% said that the level of support has been increasing
  - "Senior management has gotten religion about how important security is"
- How have budgets changed over time?
  - 88% of participants report that their security budget has increased
  - "Honestly, I have not seen a case where I asked for money and it's been turned down. It's a unique time in the field because of the hype."
  - Note: CISOs in government face steep budgetary constraints

Is all this spending going to the right places?

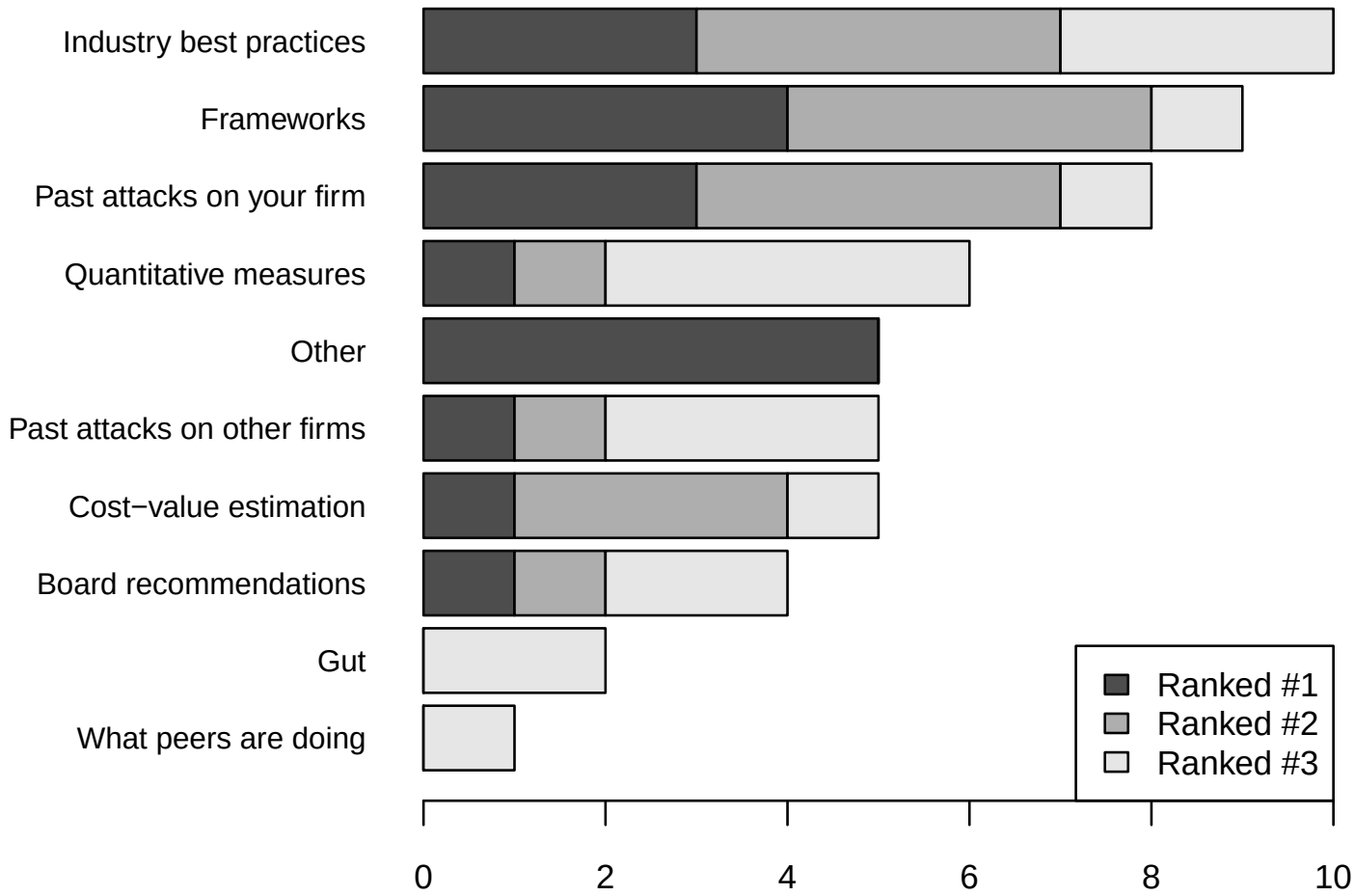
- 46% believe their organizations are spending the right amount on security, but only 7% think their peers are
- 64% said peers are spending too little
- 29% believe peers are spending too much in the wrong areas

What are the drivers of cybersecurity investment?



Responses to the question: "Please number your top 3 drivers of information security investment"

How do firms identify and prioritize threats?



Responses to the question: "Please number your top 3 prioritization approaches"

THE UNIVERSITY of TULSA

Do organizations calculate ROI to make investment decisions?

- Some firms use quantitative metrics to measure and improve operational security: counting # unpatched machines, # malware infections remediated, etc.

Do organizations calculate ROI to make investment decisions?

- Some firms use quantitative metrics to measure and improve operational security: counting # unpatched machines, # malware infections remediated, etc.
- Almost nobody used quantitative metrics to guide *investment* decisions
  - Exception: minority translated budget requests into ROI, but still expressed skepticism that these were important in driving any decision

Do organizations calculate ROI to make investment decisions?

- Some firms use quantitative metrics to measure and improve operational security: counting # unpatched machines, # malware infections remediated, etc.
- Almost nobody used quantitative metrics to guide *investment* decisions
  - Exception: minority translated budget requests into ROI, but still expressed skepticism that these were important in driving any decision
  - One CISO stated he doesn't want to sell security to the board by saying "there's a 20% chance of a $20 million breach in a given 5 years"; argument doesn't resonate

Do organizations calculate ROI to make investment decisions?

- Some firms use quantitative metrics to measure and improve operational security: counting # unpatched machines, # malware infections remediated, etc.
- Almost nobody used quantitative metrics to guide *investment* decisions
  - Exception: minority translated budget requests into ROI, but still expressed skepticism that these were important in driving any decision
  - One CISO stated he doesn't want to sell security to the board by saying "there's a 20% chance of a $20 million breach in a given 5 years"; argument doesn't resonate
  - Healthcare CISO: "in security, ROI is a fallacy. We are a cost center"

THE UNIVERSITY of TULSA

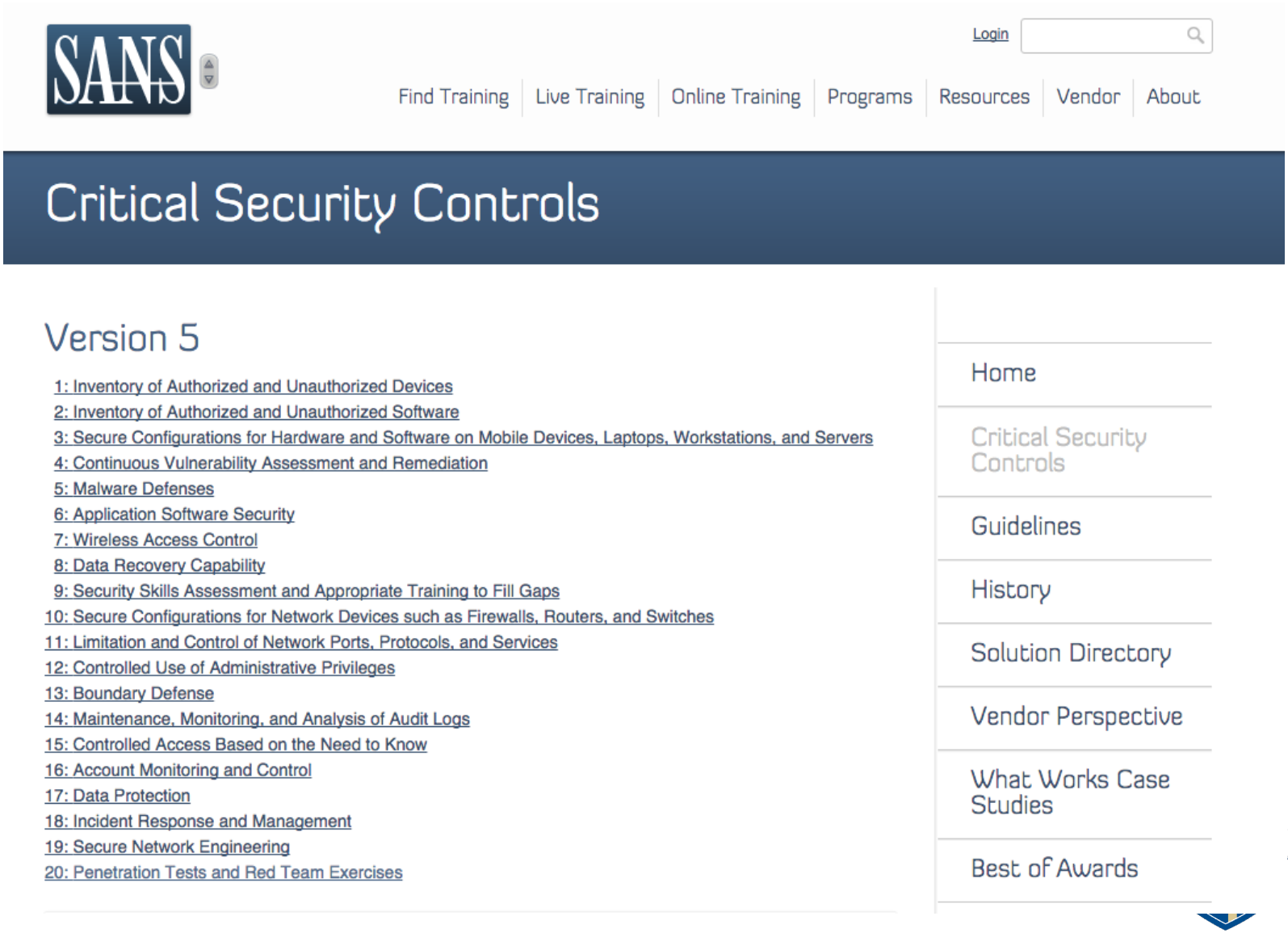
The rise of frameworks

- Few CISOs rely on quantitative risk calculations to guide investment decisions
  - Quantitative investment metrics encouraged by risk management approaches can be difficult to calculate
  - Often depend on figures that are not readily available (e.g., probability of loss, loss amount)

The rise of frameworks

- Few CISOs rely on quantitative risk calculations to guide investment decisions
  - Quantitative investment metrics encouraged by risk management approaches can be difficult to calculate
  - Often depend on figures that are not readily available (e.g., probability of loss, loss amount)
- Frameworks emphasize the *process* of managing cybersecurity without explicit regard to loss, likelihood of attack

A simple early framework: SANS 20 Critical Controls



Source: https://www.sans.org/critical-security-controls/controls

NIST Cybersecurity Framework

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

- Organized around 5 core *functions*: identify, protect, detect, respond, recover
- Each function has categories and subcategories
- Voluntary to adopt, but pushed hard by Commerce

THE UNIVERSITY of TULSA

Frameworks: good or bad?

- Frameworks are a powerful communications tool
  - CISO: frameworks make it "fairly easy to discuss and to convey to different layers of leadership"
  - CISO: frameworks clearly communicate risk rating to senior management and how much investment is needed to bring rating down to acceptable level

Frameworks: good or bad?

- Frameworks are a powerful communications tool
  - CISO: frameworks make it "fairly easy to discuss and to convey to different layers of leadership"
  - CISO: frameworks clearly communicate risk rating to senior management and how much investment is needed to bring rating down to acceptable level
- Security frameworks: the new checkbox?
  - Frameworks stimulate a broader, systematic examination of risk
  - While frameworks look more "scientific", they aren't
  - By focusing on process, rather than secure outcome, it is not clear how much the frameworks actually improve security

Markets with asymmetric information

Information asymmetries in cybersecurity markets

1. Secure software is a market for lemons
   - Vendors may believe their software is secure, but buyers have no reason to believe them
   - So buyers refuse to pay a premium for secure software, and vendors refuse to devote resources to do so
2. Lack of robust cybersecurity incident data
   - Unless required by law, most firms choose not to disclose when they have suffered cybersecurity incidents
   - Thus firms cannot create an accurate a priori estimate of the likelihood of incidents or their cost
   - Without accurate loss measurements, defensive resources cannot be allocated properly

Do CISOs view security as a market for lemons?

- We asked if organizations feel they have adequate information to manage risk and prioritize threats
  - 45% said yes; most "no's" arise from fear of "unknown unknown"
  - CISOs in finance and energy sector regularly briefed on threats by government colleagues

Do CISOs view security as a market for lemons?

- We asked if organizations feel they have adequate information to manage risk and prioritize threats
  - 45% said yes; most "no's" arise from fear of "unknown unknown"
  - CISOs in finance and energy sector regularly briefed on threats by government colleagues
- 85% of CISOs feel they have enough information to select the right security controls

Do CISOs view security as a market for lemons?

- We asked if organizations feel they have adequate information to manage risk and prioritize threats
  - 45% said yes; most "no's" arise from fear of "unknown unknown"
  - CISOs in finance and energy sector regularly briefed on threats by government colleagues
- 85% of CISOs feel they have enough information to select the right security controls
- Information sharing groups (sectoral and regional) seen as highly valuable in mitigating information asymmetries

Special challenges for government CISOs

- While management support for cybersecurity has translated to access to budget for private CISOs, this is often not the case in government

Special challenges for government CISOs

- While management support for cybersecurity has translated to access to budget for private CISOs, this is often not the case in government

1. Challenges to the budgeting process
   - Federal CISO: "Difficult to move from actionable intelligence (when I knew the bad guy was there) to legitimize procurement in something sooner than a three-year cycle. ...If I saw something in 2014 I'd have to put it in my 2017 procurement plan"
   - Any budget shift over $500K requires Congressional approval
   - Another federal CISO: "process is painfully broken"

Special challenges for government CISOs (ctd.)

2. Tensions between agency and department-level CISOs/CIOs
   - In US, CISO and CIOs appointed for departments and constituent agencies
   - In principle, department CIO/CISO oversees agency CIOs/CISOs
   - In practice, departmental-level officers have limited budgetary control, and cannot implement strategic investments across the department
   - Federal CISO: Departmental-level CISOs "don't have money, they don't have people, and they all report to CIOs. So security is subject to the imperative of keep the system up, keep the mission running, and oh yeah security if there's time and interest."

Special challenges for government CISOs (ctd.)

3. Tensions between compliance and security in oversight
   - FISMA process ensures oversight via audit for compliance to federal standards, called Security Certification and Accreditations (C&As)
   - Federal CISO: "The whole FISMA and C&A process was horrendously outdated"
     - Slowness of completing the process rendered the results immediately outdated
     - The time and budget required to comply distracts from the mission to improve security
   - Silver lining: government leaders now recognize the need to "get away from creating books that say we are safe, which is in fact taking resources away from actually making sure the government is trying to protect its networks."

Concluding remarks

- Firms are investing more in cybersecurity than ever before
- It remains to be seen if these investments will produce more secure outcomes
- Process-based frameworks preferred over outcome-based measures to guide investment
- CISOs feel that information asymmetries are not a huge problem in selecting controls
- US federal CISOs face structural impediments to achieving adequate investment in cybersecurity
- For more information, email `tyler-moore@utulsa.edu` or visit `http://tylermoore.ens.utulsa.edu`

THE UNIVERSITY of TULSA