Managing Cybersecurity Risk: Internal and External Assurance

William Dilla, Ph.D., CPA
Union Pacific / Charles B. Handy Professor
Chair, Department of Accounting
How NOT to manage cybersecurity

What we won’t talk about today
What we will do today

• Discuss research by Ivy CoB faculty and others that addresses:
  • Who cares about cybersecurity risk management?
  • What motivates cybersecurity attackers?
  • How do the cybersecurity “lines of defense” (management, information security specialists, and internal audit) work together?
• Provide brief a update on external cybersecurity assurance and reporting
• Complete and discuss a survey about other types of assurance
First, some definitions

- **Cybersecurity risk management program**
  - Addresses threats to achieving an organization’s cybersecurity objectives
  - Consistent with three categories of COSO internal control objectives (AICPA, 2017a, SOC for Cybersecurity, 1.23-1.24)
    - Operations
    - Reporting
    - Compliance

- **Assurance**
  - Internal—ISACA calls this a “cybersecurity audit” (ISACA, 2017)
  - External—AICPA SOC refers to cybersecurity risk management “assurance”
Who cares about cybersecurity risk management?

- Management
- Customers
- Investors
Do customers really care?

• Not really
• Research by ISU faculty member Rui Chen and colleagues (Valecha et al. 2016; ISU News Service, 2018)
  • Examines 2015 data breach at the U.S. Office of Personnel Management
  • Reactions on Twitter proceed through anxiety, anger, and sadness stages
  • Then they taper off, indicating either acceptance of or apathy about the breach
Do investors care?

- Voluntary disclosures about infosec policy have a positive impact on market value (Gordon, et al. 2010; Berkman, et al. 2018)
- Wang, Kannan, and Ulmer (2011) find that:
  - Firms that disclose security risk-mitigation factors are less likely to report breaches
  - When breaches do occur, risk-mitigating firms have smaller negative market reactions
- Amir, et al. (2018) find that
  - Disclosed attacks result in an 0.7% decline in equity values, on average
  - Undisclosed attacks result in a 3.6% decline
Another reason that management should care

- Yen, et al. (2018) find that
  - Audit fees are higher after an information security breach
  - The following mitigate the audit fee increase
    - The audit firm’s industry experience
    - Big 4 firms
    - Length of audit firm tenure
What motivates cybersecurity attackers?

• Not much objective information out there
  • How do you interview anonymous attackers?
• “MICE” framework (Dorminey, et al. 2010, 2012)
  • Money
  • Ideology
  • Coercion
  • Ego / entitlement
Do trade secrets increase the risk of attack?

- Ettredge, Guo, and Li (2018) find that firms with 10-K disclosures of trade secrets are more likely to be breached.

- Results are stronger for:
  - Newer firms
  - Firms with fewer employees
  - Firms operating in less concentrated industries
Cybersecurity “Lines of Defense” Research

- Three studies
  1. Interviews with IT security managers and internal auditors
  2. Survey of IT security professionals about perceived security outcomes
  3. Survey of internal auditors, external auditors and consultants about actual security outcomes

Also in ISACA (2017)
1. The relationship between internal audit and information security: An exploratory investigation (Steinbart, Raschke, Gal, and Dilla, 2012)

- Respondents are internal auditors and IT personnel from:
  - Two large state universities
  - One mid-sized private university
  - One for-profit higher ed institution

![Diagram showing the relationship between internal audit and information security.](image)
2. Information security professionals’ perceptions about the relationship between the information security and internal audit functions (Steinbart, Raschke, Gal, and Dilla, 2013, 2014)

Information security effectiveness: respondent perceptions of whether information security is improving
3. The influence of a good relationship between the internal audit and information security functions on information security outcomes (Steinbart, Raschke, Gal, and Dilla, 2018)

- Indicators of information security effectiveness
  - Leading
    - Security-related IC weaknesses reported to the Board of Directors
    - Employee non-compliance with IT policies
  - Lagging
    - Security incidents detected and stopped before causing material harm
    - Security incidents detected and stopped after causing material harm
Influence of IA / InfoSec Relationship on Outcomes

- Two types of influence
  - Collaborative detection
  - Knowledge transfer
- Effects on leading indicators
  - Collaborative detection effect always positive
  - Knowledge transfer may taper off over time
  - Can’t make a directional prediction
- Effects on lagging indicators
  - Should have a positive influence on number of attacks detected before causing material harm
  - Can’t make a directional prediction on number of attacks detected after causing material harm
What we did

• Surveyed AICPA IMTA section members: 110 usable responses

• Internal audit respondents rated their organization’s information security program ("A" through "F")

• External audit / consultant respondents were told to respond for a client with either high ("A" or "B") or low ("C," "D," or "F") quality information security
Antecedents of a Good IA / InfoSec Relationship

- These factors positively influence the IA / InfoSec relationship
  - Whether CISO reports independently of CIO
  - Top management support for information security
- However, neither has a direct effect on security outcomes
Leading indicator results

IA / InfoSec Relationship Quality → Leading InfoSec Quality Indicators → Controls

- %age of IT Function Time Devoted to InfoSec
- Number of Employees
Lagging indicator results

- IA / InfoSec Relationship Quality
- Incidents Detected Prior to Causing Harm
  - Controls
    - %age of IT Function Time Devoted to InfoSec
    - Number of Employees
  - Incidents Detected After Causing Harm
    - Controls
      - %age of IT Function Time Devoted to InfoSec
      - Number of Employees

Ivy College of Business
Department of Accounting
Summary

• All three “lines of defense” are important in assuring the success of a cybersecurity risk management program

• Top management indirect effects
  • Facilitate a good relationship between IA and the InfoSec functions
  • Provide adequate resources to IT function for information security
Summary

- Percentage of time spent on information security
  - Does not affect leading indicators
  - Increases number of stopped incidents / decreases number of harmful incidents
- Relationship between IA and information security
  - Positive influence on leading indicators
  - Increases number of stopped incidents
  - Also increase number of incidents detected after causing harm
    - This is not necessary a bad thing. Why?
- Results show different roles of InfoSec vs. the IA function
External Cybersecurity Assurance

• AICPA Issued SOC for Cybersecurity May 2017
• Intent is to provide an attestation report for a “broad range of users”
• Contrasts to SOC2 reports, which are intended for service organization users (AICPA, 2017b)
• Provider reports on whether:
  • The entity’s description of its cybersecurity risk management program is in accordance with the description criteria
  • The controls implemented within the program were suitably designed to achieve the entity’s cybersecurity objectives
• Note the carefully defined scope
  • Compare to PCAOB internal control over financial reporting opinion
• No real “updates” since SOC issuance
Updated disclosure requirements

• New SEC (2018) guidance includes
  • Updated disclosure guidelines regarding cybersecurity risks and material events
  • Specifies requirement for disclosure controls and procedures related to cybersecurity
  • Consideration of effects of cybersecurity risks and incidents on financial statements

• So far, no separate cybersecurity assurance required
• Center for Audit Quality (CAQ, 2018) has issued a guide regarding current audit implications
References

AICPA, 2017a, Guide: Reporting on an entity’s cybersecurity risk management program and controls.


