CYBERSECURITY AND THE ACCOUNTING PROFESSION

A DISCUSSION OF ETHICAL IMPLICATIONS

Prepared for discussion with IESBA's Technology Task Force and Working Group

Thomas G. Calderon, Ph.D.
Professor of Accounting
The University of Akron
tcalder@uakron.edu
330-324-0749

July 27, 2021

Why emphasize ethics?

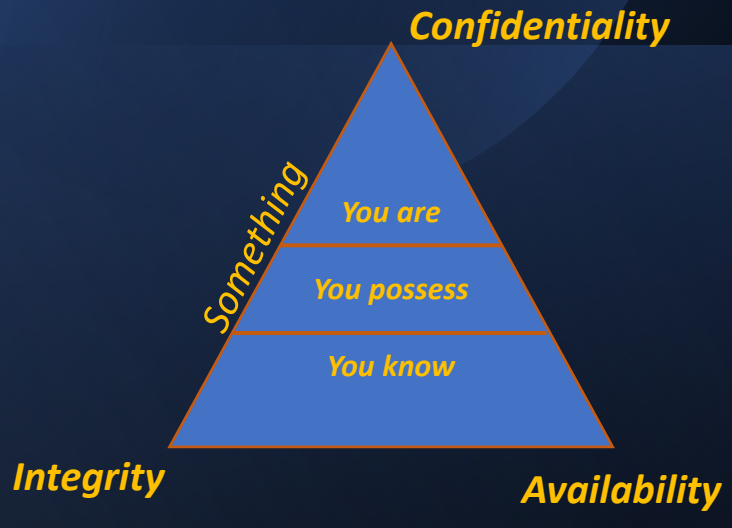
- Much has been written about cybersecurity. The literature emphasize such topics as:
  - Cybersecurity and the public accountant
  - Cybersecurity and the role of the internal auditor and accountant
  - Security in the cloud
  - Cybersecurity authentication and holistic approaches to security
  - Cybersecurity risk disclosures
  - Risks, incentives and behaviors in cybersecurity
- Very little has been written about the ethical implications of cybersecurity for the accounting profession

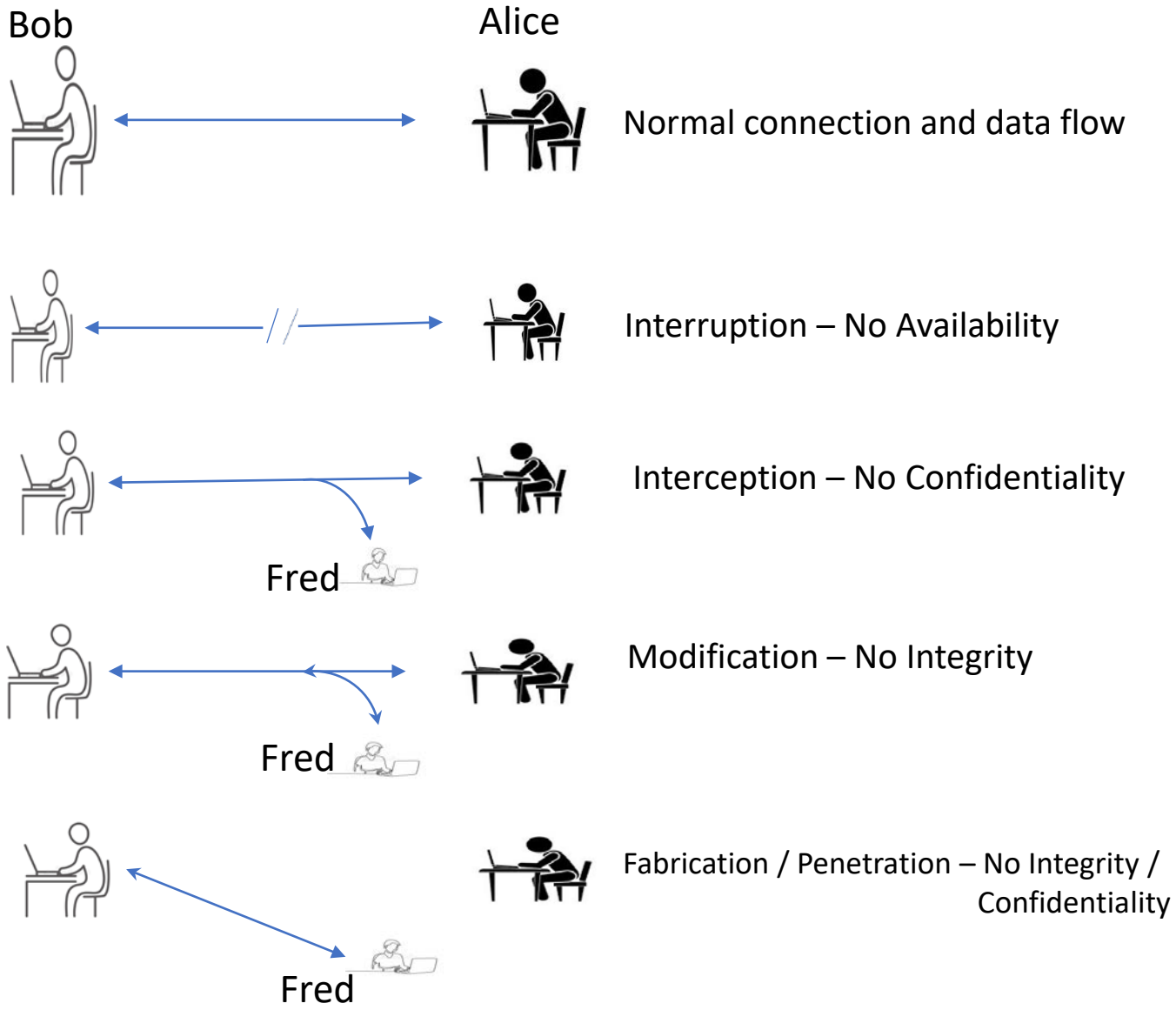
Why focus on cybersecurity – some statistics from Veronis?

https://www.varonis.com/blog/cybersecurity-statistics/

- “The worldwide information security market is forecast to reach $170.4 billion in 2022. (Gartner)
- 88% of organizations worldwide experienced spear phishing attempts in 2019. (Proofpoint)
- 68% of business leaders feel their cybersecurity risks are increasing. (Accenture)
- On average, only 5% of companies’ folders are properly protected. (Varonis)
- Data breaches exposed 36 billion records in the first half of 2020. (RiskBased)
- 86% of breaches were financially motivated and 10% were motivated by espionage. (Verizon)
- 45% of breaches featured hacking, 17% involved malware and 22% involved phishing. (Verizon)
- Between January 1, 2005, and May 31, 2020, there have been 11,762 recorded breaches. (ID Theft Resource Center)
- 95% of cybersecurity breaches are caused by human error. (Cybint)
- The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%. (Symantec)
- An estimated 300 billion passwords are used by humans and machines worldwide. (Cybersecurity Media)”

Cybersecurity fundamentals

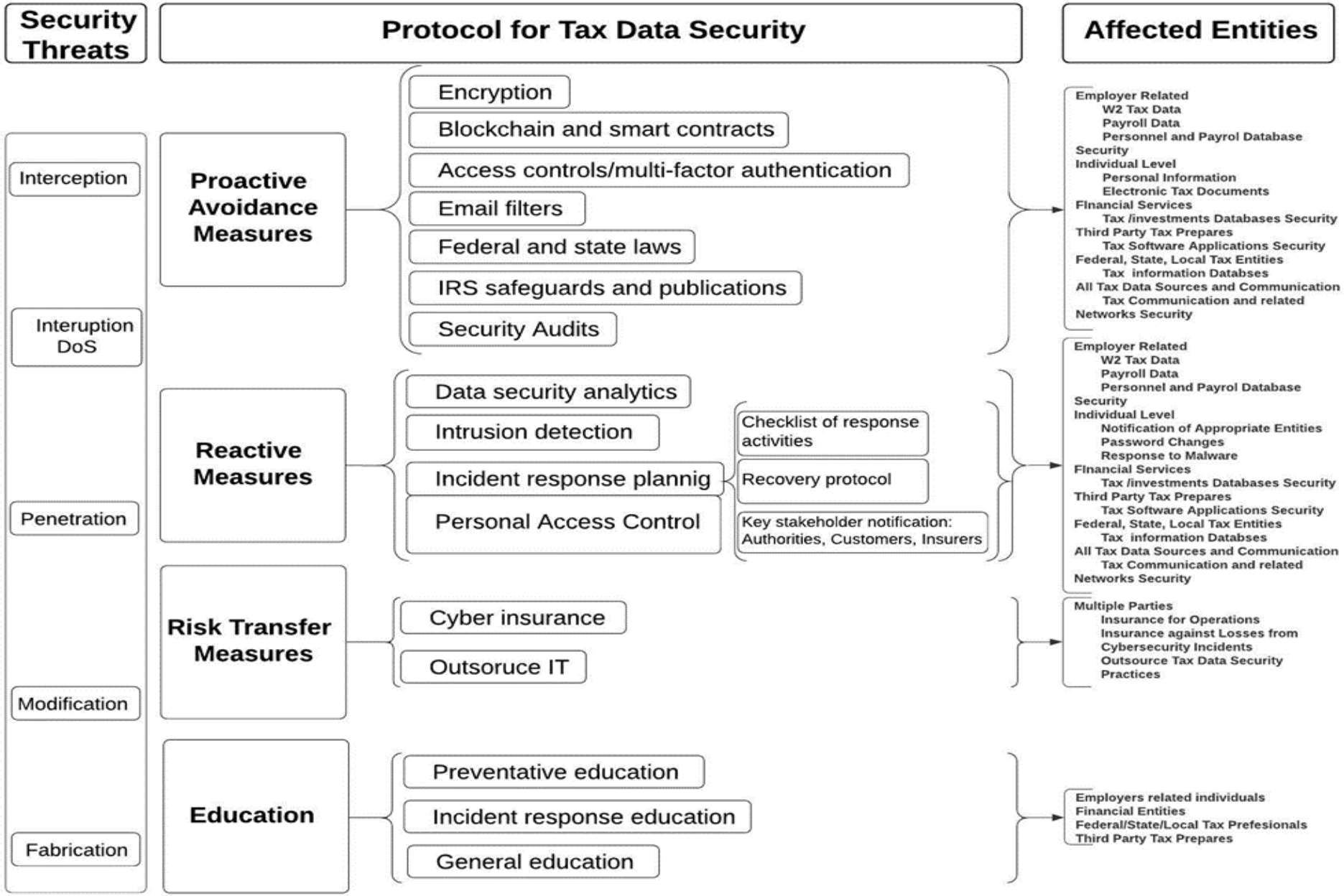




Management of Cybersecurity Risk

- Four categories of measures used to managing cybersecurity risk:
  - proactive measures
  - reactive measures
  - risk transference
  - Education
- Doing nothing is always an “option” but the average cost of a data breach is about $3.86 million
  - Not a financially feasible option
  - High risk of financial ruin

Illustrating cybersecurity risk management – a tax example from Calderon et al. 2021



Some observations about contemporary cybersecurity threats

- Remote working accentuates cybersecurity risks –
  - blurred lines between personal and business information systems
  - potentially new access points for malicious actors
  - Potentially less secure and more vulnerable environments
- The Internet of Things (IoT) add vulnerability –
  - creating more entry points for mischief
  - Prediction - more than 8 IoT for each living person in the world by 2026
- Ransomware attacks increasing in frequency and cost –
  - costly and deadly with the first human death related to ransomware occurring in 2020 when a German Hospital was locked out of its systems resulting in the death of a female patient who had to be transported to a neighboring hospital 20 miles away.
  - marriage of digital currency and ransomware creating perfect storm scenarios
  - Colonial Pipeline, JBS foods and Axa are high profile examples
- Ubiquity of cloud services increase threats and vulnerability –
  - rapid expansion of remote work make this trend particularly risky for business with growing exposure in such areas as:
    - regulatory compliance across jurisdictions
    - pressure on available cloud computing expertise
    - cloud migration
    - blurred lines between data in the cloud and data on personal computers
    - increasing vulnerability of systems as possible access points for attackers multiply

- Adapted from - https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends

Some observations about contemporary cybersecurity threats

- Social engineering attacks getting smarter –
  - With more people working remotely, social engineering attacks are becoming more personal and more focused.
  - *Phishing, whaling and smishing* attacks are among new words that are expanding the contemporary lexicon.
- Greater legal and regulatory demand for data privacy –
  - Data privacy is increasingly being prioritized
  - Patchwork of federal and state privacy laws and data breach reporting requirements
  - In contrast to the US, EU General Data Protection Regulation (GDPR) is a comprehensive privacy legislation that applies across sectors and to companies of all sizes.
- Multi-factor authentication improving –
  - Becoming more commonplace
  - Increasing reliance on something that “you know” and something that “you own”

- Adapted from - https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends

Some observations about contemporary cybersecurity threats

- Mobile cybersecurity is the new battlefront
  - Proliferation of mobile apps
  - Growing reliance on mobile password managers
  - Integration of something that “you know” and something that “you are”
- Data poisoning is a growing and potentially highly disruptive threat
  - polluting a machine learning model's training data
  - High failure rates and/or fraudulent guidance
  - Potential extension could be poisoning financial reporting data
- Focusing attacks on service providers
  - “On Saturday morning, the information technology company Kaseya confirmed that it had suffered a “sophisticated cyberattack” on its VSA [Virtual System Administrator] software — a set of tools used by IT departments to manage and monitor computers remotely. The company said that only about 40 customers had been affected.
  - But because Kaseya’s software is used by large IT companies that offer contract services to hundreds of smaller businesses, the hack could have spread to thousands of victims. Kaseya told all of its nearly 40,000 customers to disconnect their Kaseya software immediately. The cybersecurity firm Huntress Labs said it had tracked 20 IT companies, known as managed-service providers, that had been hit. More than 1,000 of those companies’ clients, mostly small businesses, also had been affected by the hack, Huntress Labs said on Reddit.
  - A major grocery chain in Sweden said Saturday that its IT provider had been hit by an attack and that its cash registers were locked up. It had to shut down hundreds of stores, the company, Coop Sweden, said on its Facebook page.” July 2, 2021.

https://www.washingtonpost.com/technology/2021/07/02/kaseya-ransomware-attack/

Cybersecurity risk disclosures

Gao, Calderon & Tang 2020

International Journal of AIS

- The US SEC expects registrants to disclose cybersecurity risks (2011 and 2018 Guidance)
- Two most commonly disclosed cybersecurity risks are
  - risks of service/operation disruption and
  - risks of data breach.
- Item 1A of the 10-K Report is the most commonly used disclosure location, but some companies also use Items 1 and 7 to disclose regulation risks and cyber incidents, respectively.
- The length of cybersecurity risk disclosures increased linearly during the period 2004 to 2202.
- Cybersecurity risk disclosure is associated with the issuance of SEC guidance (2011 and 2018), industry, trends in overall cybersecurity risks in the general environment, company size, and prior cybersecurity breach incidents.
- There is more disclosure but disclosures have also become more difficult to read in general.
- Global enterprises that file 20-F reports tend to have longer and clearer cybersecurity risk disclosures than their US counterparts (Calderon & Gao 2021 *Journal of Emerging Technologies in Accounting*)
- SEC uses its staff comment letter process to nudge registrants to make better cybersecurity risk disclosures (Calderon & Gao 2021 Unpublished Working Paper).

Cybersecurity and ethics

IESBA CODE

- **THE FUNDAMENTAL PRINCIPLES**
  - Integrity
  - Objectivity
  - Professional Competence and Due Care
  - Confidentiality
- PROFESSIONAL BEHAVIOR
- INDEPENDENCE

Cybersecurity and ethics

Many issues with implications for professional accountants can arise in the management and disclosure of cybersecurity risk.

Perspective	Possible Issues of Concern With Professional Ethics Implications
Management and Preparer's Perspective	• Violation of laws and regulation related to cybersecurity • Failure to disclose cybersecurity incidents • Deficiencies in cybersecurity risk disclosures • Failure to consider the impact of cybersecurity policies and practice on internal control • Misleading response to an SEC Comment letter • Failure to provide or support training for staff and professionals in the area of cybersecurity

Cybersecurity and ethics

Many issues with implications for professional accountants can arise in the management and disclosure of cybersecurity risk.

Perspective	Possible Issues of Concern With Professional Ethics Implications
Internal Auditor's Perspective	• No assessment of the effectiveness of cybersecurity in the financial reporting system • Material participation in the design, creation and execution of cybersecurity policies • Unaware of cybersecurity risk management measures deployed by the company • Offers no cybersecurity risk training for staff and professionals • Shares information about a cybersecurity breach with the press • Shares information about a cybersecurity breach with a family member • Sells stocks after a cybersecurity breach but before the company makes information about the breach public.

Cybersecurity and ethics

Many issues with implications for professional accountants can arise in the management and disclosure of cybersecurity risk.

Perspective	Possible Issues of Concern With Professional Ethics Implications
Independent Auditor Perspective	• Audits financial statements after advising client on cybersecurity risk management processes • Member of the audit firm who serves on the audit team is also contracted by the client to provide cybersecurity services. • Provides no cybersecurity risk training for staff and professionals • Evaluates internal control but excludes cybersecurity from the scope of the evaluation • Discloses confidential information about a cybersecurity breach at an audit client to a partner in the audit firm • Relies on an incompetent third party for SOC audit of general controls over the revenue and expenditure cycles • Advises a client to pay a hacker who orchestrated a ransomware attack on the financial reporting system after the fiscal year end but before publication of financial statements in order to assure a timely audit • Promotes the audit firm as a firm with a perfect record in helping clients prevent cybersecurity attacks

Cybersecurity and ethics - conclusion

Ethical implications can be broad and touch all aspects of the code.

Cybersecurity attacks can be surreptitious. No one may know of or feel the harm while they are in progress.

Because professional accountants are not generally trained in the area of cybersecurity risk, control and assurance, it is not clear whether they are familiar with the potential intersection between the cybersecurity risk and each of the following aspects of the code:

- Integrity
- Objectivity
- Professional Competence and Due Care
- Confidentiality
- Professional Behavior
- Independence

- The implications of not being fully aware of that overlap can be costly for individual accounting professionals and the profession as a whole.

Questions?

Thomas G. Calderon, Ph.D.
Professor of Accounting
The University of Akron
tcalder@uakron.edu
330-324-0749