Proactive Risk: Managing, Mitigating, and a Case Study in Election Security

Natalie M. Scala, Ph.D.

NATO 15th Operations Research and Analysis Conference

October 2021

TOWSON UNIVERSITY
Supply Chain Management

Cyber Risk: Reactive to Proactive

TOWSON UNIVERSITY | Supply Chain Management

- User problem (threat) vs. data problem (risk)
  - Insiders, cyber concerns, etc.
- Shift from reactive to proactive policies to manage
- Reactive: Protection and privacy of data itself
  - Secure email, web monitoring, phishing, breaches
- Proactive: Prevention by means of a centralized policy or process
  - Working to prevent before occur

(c) Natalie M. Scala, 2021

Metrics: Two Definitions

TOWSON UNIVERSITY | Supply Chain Management

- Cybersecurity: Best practices, predictive measures
- Analytics: Descriptive
- Very hard to define
- Great interest to the intelligence community
- Definitions align with approaches and how define security space
- Level of risk
  - Willing to take on?
  - Level needed?
  - What is appropriate?

(c) Natalie M. Scala, 2021

Insiders are Part of the Solution

TOWSON UNIVERSITY | Supply Chain Management

- Non-malicious insiders become part of the solution
  - Empower with solutions
  - Positive feedback loops
- Break bottlenecks of workarounds
- “See something, say something”
- Human behavior drives degree of inherent risk
  - Approach questions, interact with systems, behaviors
  - Coach from on the ground
  - How does your team work?
- NSA Hard Problem

(c) Natalie M. Scala, 2021

Consider Threat Systemically

- Cyber, physical, insider
- Human behavior is only one approach

(c) Natalie M. Scala, 2021

Case Study: Election Security

TOWSON UNIVERSITY | Supply Chain Management

- U.S. Help America Vote Act (2002): Sweeping reforms to voting processes
  - Voting systems, voter access
  - Punch cards
- Department of Homeland Security (2017): 21 states target of attacks to voting systems during the 2016 Presidential Election
- Senate Intelligence Committee (2019): Election systems in all 50 states targeted in 2016
- Robert S. Mueller, III (2019): Interference ongoing
- DHS (2017): Election infrastructure is critical infrastructure
  - Voting systems, storage of ballots and equipment, associated infrastructure
  - Government Facilities sector

(c) Natalie M. Scala, 2021

Systemic Threats

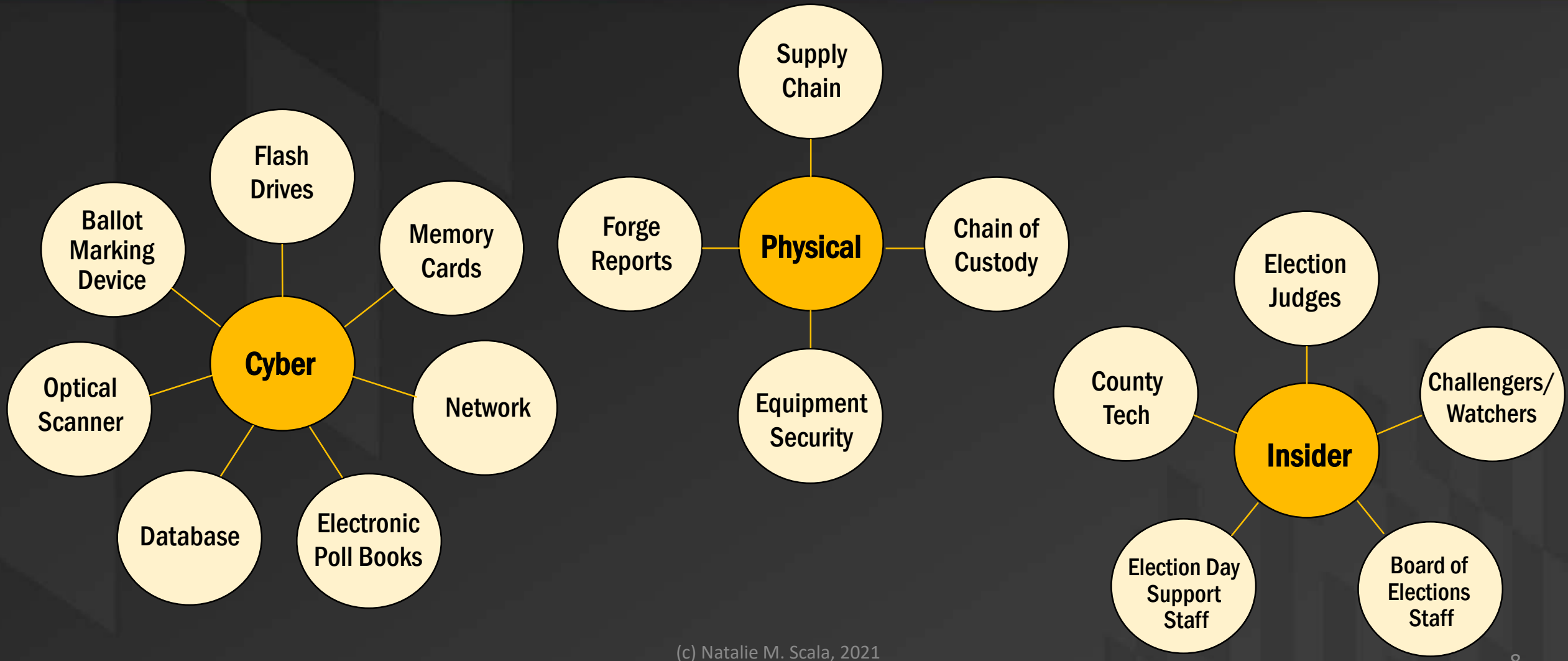
TOWSON UNIVERSITY | Supply Chain Management

- First academic team to define threats systemically in elections
- Framing extends beyond elections
- Cyber
  - Digital machines and media
  - Regardless of Internet connection
- Physical
  - Tampering with or disrupting equipment
- Insider
  - Adversaries and insiders
  - Simple, honest mistakes
  - Deliberate actions with ill-harm effects

(c) Natalie M. Scala, 2021

Sources of Threat

TOWSON UNIVERSITY | Supply Chain Management



(c) Natalie M. Scala, 2021

What about COVID-19?

TOWSON UNIVERSITY | Supply Chain Management

- Crowding, lines, sick poll workers are problems
- Constant state of flux, plans changing, shifts in process
  - 40% of states had process change in primary
  - 47 states continued with expanded mail for General Election
- Need access in place
  - Safe, socially distant methods of voting
- Attacks on legitimacy of mail votes
  - Political discourse, (mis)information
  - Social media, instructions, messaging
- What does the data say?
  - Mix of mail with in-person voting adds complexity
  - Harder for adversary to infiltrate, less impact or value

(c) Natalie M. Scala, 2021

Who was Targeted in 2016?

TOWSON UNIVERSITY | Supply Chain Management

	Targeted	Non-Targeted
# standardized states + D.C.	9	7
# non-standardized states + D.C.	12	23
% standardized equipment	56.25%	43.75%
% non-standardized equipment	34.29%	65.71%
% voting red in 2016	52.38%	60.00%
% voting blue in 2016	47.62%	40.00%

- Center for American Progress report (2018)
- Targeted status in 2016 via DHS (*The Washington Post*, 2017)
- Data coded and available at www.drnataliescala.com/projects

(c) Natalie M. Scala, 2021

Attack Trees and Risk Analysis

TOWSON UNIVERSITY | Supply Chain Management

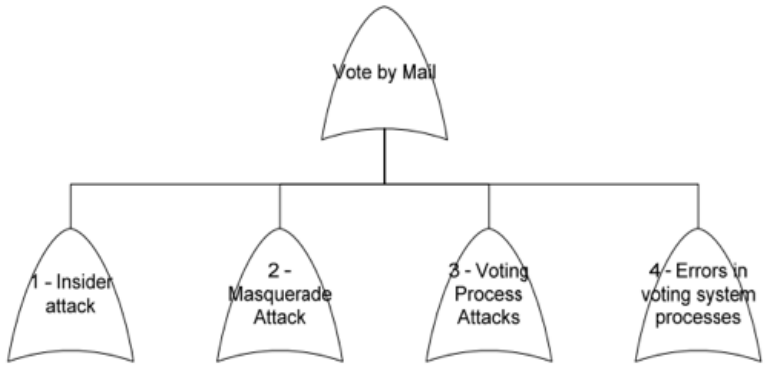
- Attack tree is inventory of risks
  - Does not identify strength or likelihood
  - Threats and scenarios: Systemic sources
- Decompose complex actions into hierarchical levels
- Graphic representation of security problem
- EAC data: Much has changed
  - 8 states fully or mostly mail voting
  - COVID-19
  - Adaptive adversary

(c) Natalie M. Scala, 2021

Vote by Mail Attack Tree (EAC, 2009)

TOWSON UNIVERSITY | Supply Chain Management

Vote by Mail Threat Tree – Graphic

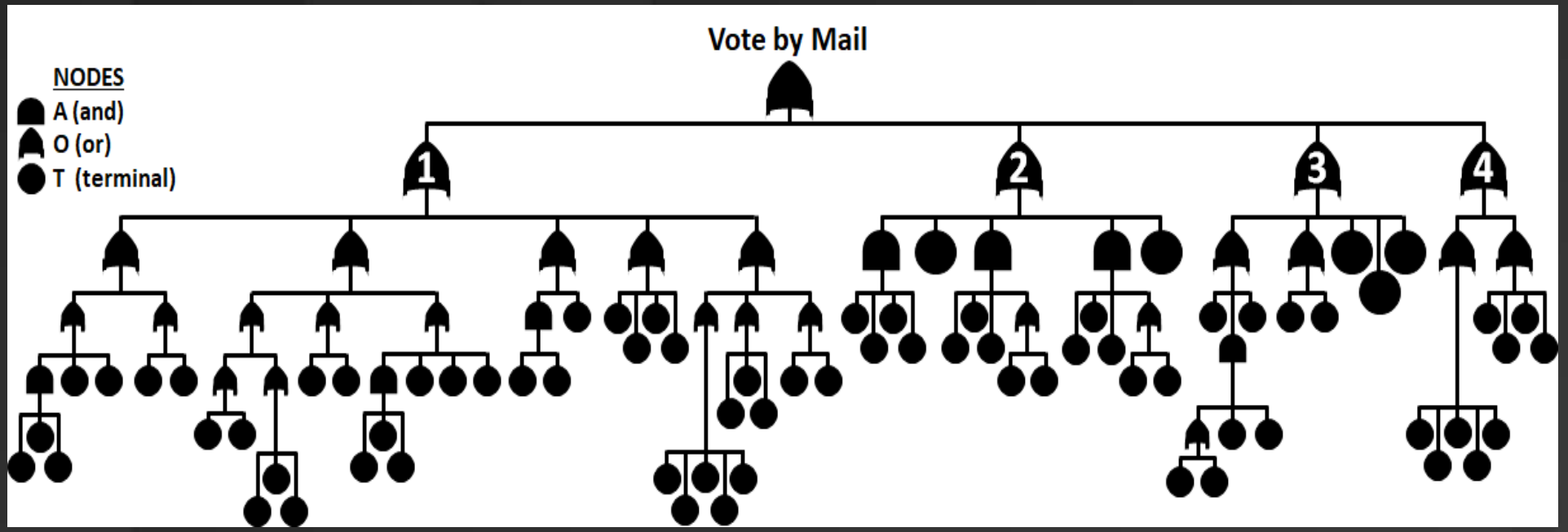


5-1 Vote by Mail Overview

node type - outline number - threat action			
O	1	Insider attack	
O	1.1	Edit Marked Ballots	
O	1.1.1	Edit at Local Elections Office	
A	1.1.1.1	Edit During Duplication	
T	1.1.1.1.1	Form Collaboration of PWs	
T	1.1.1.1.2	Gain Exclusive Access to Ballots	
T	1.1.1.1.3	Mark under/overvotes or change votes	
T	1.1.1.2	Edit During Counting	
T	1.1.1.3	Edit During Other Handling	
O	1.1.2	Edit in Transit	
T	1.1.2.1	Edit in Post Office	

- Insider threats, external threats, voter error
- Hierarchy consists of *or* (O), *and* (A), *terminal* (T) nodes

Vote by Mail Attack Tree (EAC, 2009)



- Threat scenarios
  - Insider = 32
  - External = 16
  - Voter error = 9
  - Total = 57

(c) Natalie M. Scala, 2021

Investigating Attack Tree Revisions

TOWSON UNIVERSITY | Supply Chain Management

Needs

- Pandemic implications
- Threats to critical infrastructure
- Adaptive adversary

Validation

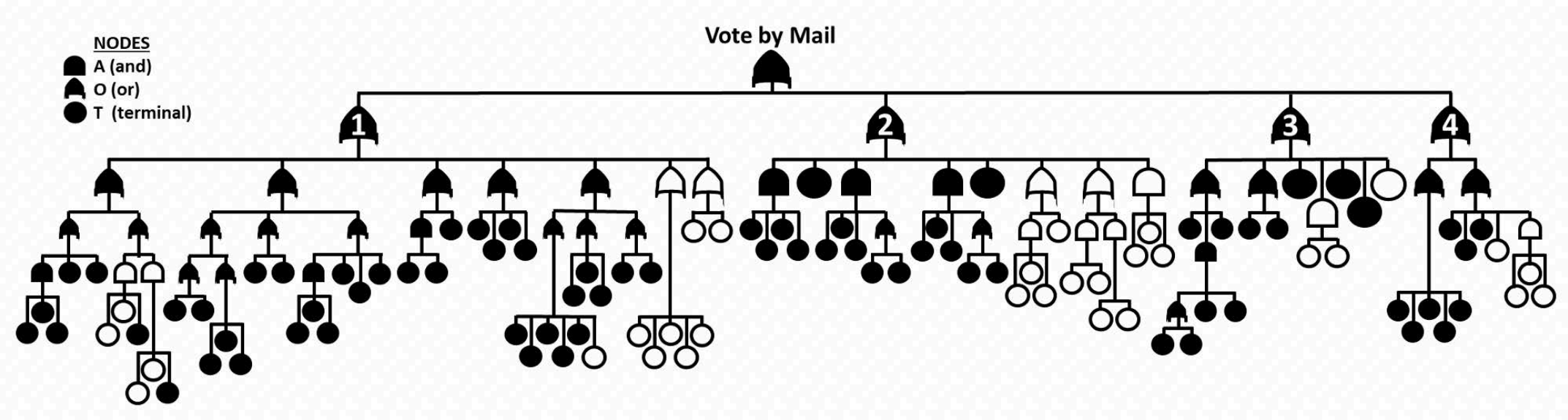
- Boards of Elections
  - Maryland counties

Sources of data

- Mainstream, non-partisan news articles
  - January through August 2020
- Bipartisan or non-political think tanks
- Academic centers
- Voter instruction sheets
- State-created documentation
- Price, et al. (2019)
- Locraft, et al. (2019)
- Scala, et al. (2020) & modules
- Poll worker training manuals

(c) Natalie M. Scala, 2021

Updated Attack Tree



- 30 new threats
- Threat scenarios
  - Insider = 40
  - External = 23
  - Voter error = 10

(c) Natalie M. Scala, 2021

What are the New Threats?

TOWSON UNIVERSITY | Supply Chain Management

Node	Vulnerability	Branch
X_{73}	Form collaboration with mail worker and acquire access	Insider
X_{74}	Break into post office	Insider
X_{75}	Form collaboration with mail worker and acquire access	Insider
X_{76}	Break into intermediate mail room	Insider
X_{77}	Manipulate return envelope	Insider
X_{78}	Misallocate polling or drop-box locations	Insider
X_{79}	Provide regional mail-in voting misinformation	Insider
X_{80}	Hinder or suppress regional postal services	Insider
X_{81}	System outage	Insider
X_{82}	Name deliberately misspelled on ballot	Insider
X_{83}	Paper ballot scanner hacked	Insider
X_{84}	Vote denied or altered	Insider
X_{85}	Identify target	External
X_{86}	Acquire access to drop box	External
X_{87}	Alter marks and return their ballots	External
X_{88}	Destroy drop box	External
X_{89}	Gain exclusive access to ballot storage	External
X_{90}	Alter marks and return to storage	External
X_{91}	Gain exclusive access to ballot storage	External
X_{92}	Steal/destroy ballots	External
X_{93}	Steal blank ballot from mailbox	External
X_{94}	Mark and return their ballot	External
X_{95}	Defeat signature check	External
X_{96}	Paper ballot scanner hacked	External
X_{97}	Vote denied or altered	External
X_{98}	Invalid ID card attack	External
X_{99}	Error in instructions	Voter error
X_{100}	Unclear assistance instructions when not required	Voter error
X_{101}	Ballot says ID required when not required	Voter error
X_{102}	Expired Voter ID	Voter error

(c) Natalie M. Scala, 2021

Strength or Likelihood of Threat

TOWSON UNIVERSITY | Supply Chain Management

- Consider utility on three dimensions
  - Attack cost (AC) u_1
  - Technical difficulty (TD) u_2
  - Discovering difficulty (DD) u_3
- Terminal nodes
- Criteria adapted from Du and Zhu (2013)

Attack Cost (AC)		Technical Difficulty (TD)		Discovering Difficulty (DD)	
Grade	**Standard**	**Grade**	**Standard**	**Grade**	**Standard**
5	Severe consequences likely	5	Extremely difficult	1	Extremely difficult
4	High consequences likely	4	Difficult	2	Difficult
3	Moderate consequences likely	3	Moderate	3	Moderate
2	Mild consequences likely	2	Simple	4	Simple
1	Little to no consequences likely	1	Very simple	5	Very simple

(c) Natalie M. Scala, 2021

Assessing Utility: Delphi Method

(c) Natalie M. Scala, 2021

Calculating Relative Likelihood

TOWSON UNIVERSITY | Supply Chain Management

- Relative likelihood for each terminal node X_j:

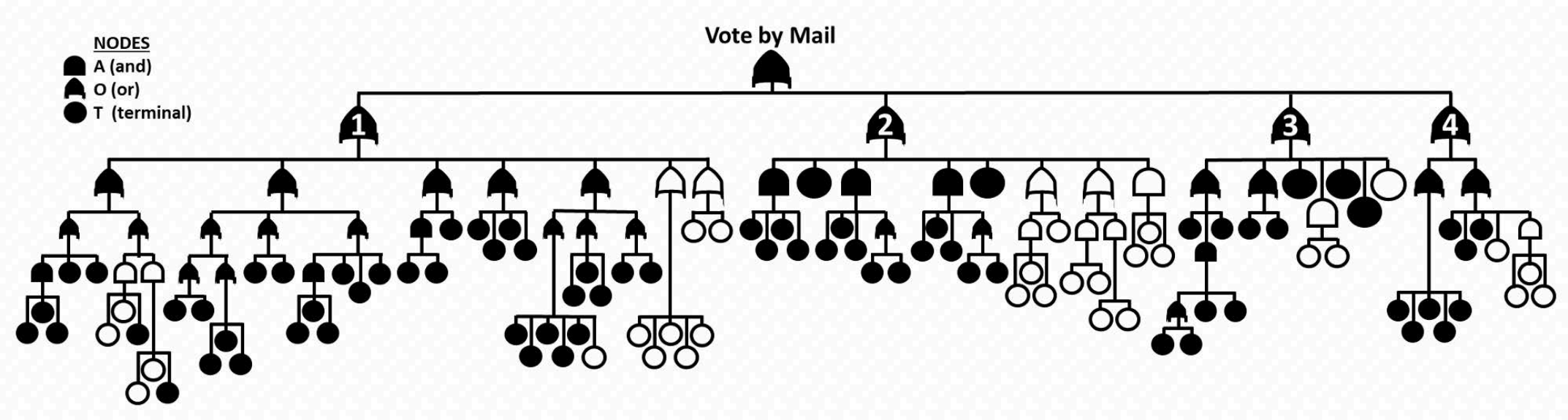
$$P(X_j) = w_1 u_{1j} + w_2 u_{2j} + w_3 u_{3j}$$

  - $j \in \{1, 2, \dots, n\}$, n terminal nodes
  - $w_k, k \in \{1, 2, 3\}$, weight assigned to utility function k; $\sum w_k = 1$
    - $w_k = {}^1/_3 \; \forall k$
  - $u \in [0, 1]$, using scale factor (0.2) to convert ordinal scales

Terminal Node	AC	TD	DD	Relative Likelihood	Terminal Node	AC	TD	DD	Relative Likelihood
T 1.1.1.1.1 (X_1)	4	2	2	0.08	T 2.1.3 (X_{40})	5	2	3	0.07
T 1.1.1.1.2 (X_2)	4	3	2	0.07	T 2.1.4 (X_{41})	4	2	1	0.12
T 1.1.1.1.3 (X_3)	3	4	2	0.07	T 2.2 (X_{42})	5	2	2	0.08
T 1.1.1.2 (X_4)	5	3	3	0.06	T 2.3.1 (X_{43})	4	3	3	0.06
T 1.1.1.3 (X_5)	3	4	3	0.06	T 2.3.2 (X_{44})	4	2	3	0.07

(c) Natalie M. Scala, 2021

What about Scenarios?



- Threat scenarios
  - Insider = 40
  - External = 23
  - Voter error = 10
  - Total = 73

Relative Likelihood for Scenarios

TOWSON UNIVERSITY | Supply Chain Management

- For an attack scenario $S_i = (X_{i1}, X_{i2}, \ldots, X_{iN})$
  - AND structure: $P(S_i) = P(X_{i1})P(X_{i2}) \ldots P(X_{iN})$
  - OR structure: $P(S_i) = P(X_{i1})$
- Least likely: High cost, difficult to pursue, easy to discover

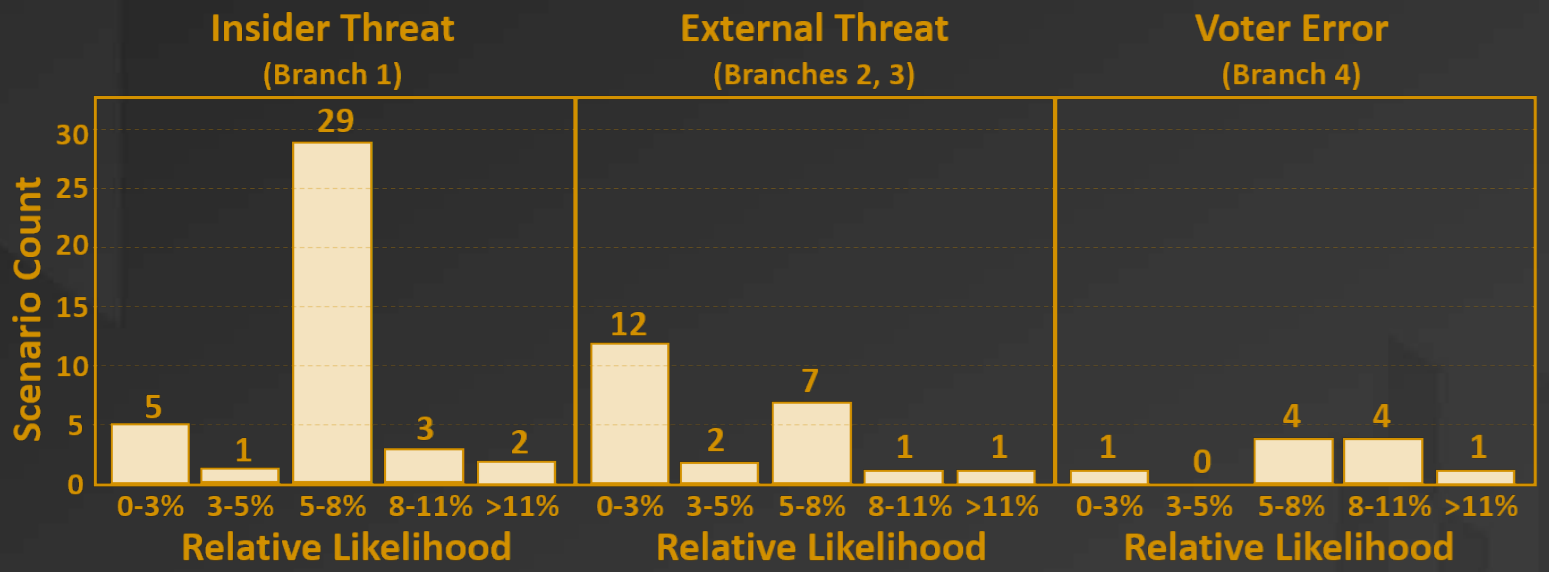
Attack Sequence	Leaf Node(s)	Relative Likelihood	Attack Sequence	Leaf Node(s)	Relative Likelihood
S_1	X_1, X_2, X_3	0.0004	S_{38}	X_{82}	0.0600
S_2	X_4	0.0600	S_{39}	X_{83}	0.0600
S_3	X_5	0.0600	S_{40}	X_{84}	0.0700
S_4	X_{73}, X_{74}, X_6	0.0002	S_{41}	X_{38}, X_{39}, X_{40}, X_{41}	0.0000

(c) Natalie M. Scala, 2021

Scenario Likelihood

TOWSON UNIVERSITY | Supply Chain Management

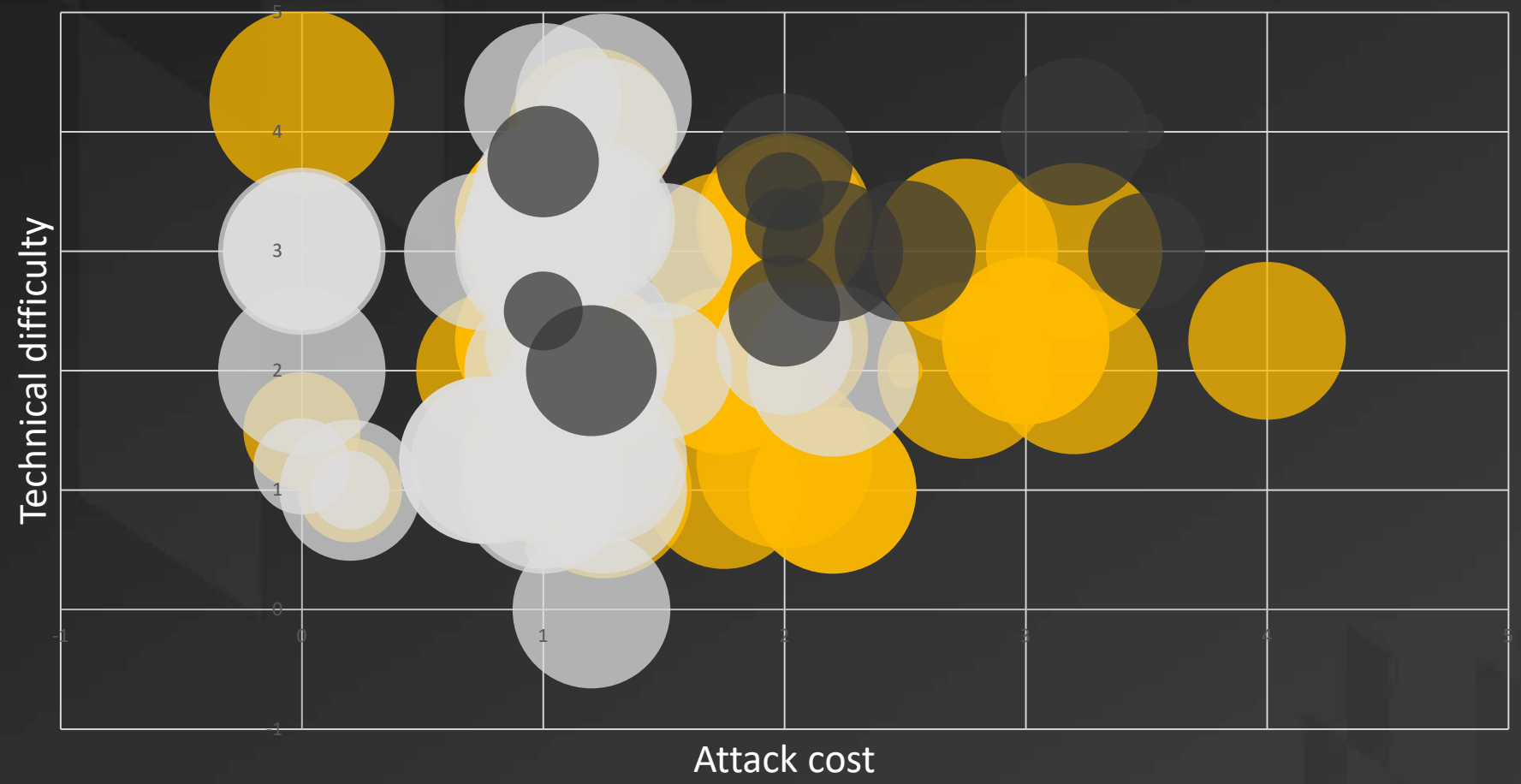
- Insider: Majority of scenarios
- External: Very low relative likelihood
  - External actors may not be interested or incentivized
- Voter error: Only 13.7% of total scenarios



(c) Natalie M. Scala, 2021

Threat Impact on Mail Voting

TOWSON UNIVERSITY | Supply Chain Management



- Considering attack cost, technical difficulty, discovering difficulty
- Yellow = insider threats, white = external threats, black = voter error threats

(c) Natalie M. Scala, 2021

Threats of Most Concern

TOWSON UNIVERSITY | Supply Chain Management

Scenario	Threat		Relative Likelihood	Branch
S_7	X_9	Errant failed signature	0.12	Insider
S_{12}	X_{14}	Accidental loss	0.10	Insider
S_{23}	X_{28}	Fail to stuff envelope	0.11	Insider
S_{32}	**X_{36}**	**Lost in destination mailroom**	**0.13**	**Insider**
S_{47}	X_{53}	Malicious "messenger ballots"	0.10	External
S_{58}	**X_{61}**	**Debate and vote parties**	**0.12**	**External**
S_{64}	**X_{65}**	**Failure to sign correctly**	**0.13**	**Voter Error**
S_{66}	X_{67}	Failure to bundle correctly	0.11	Voter Error

- No new threats identify as high concern
- *Quick move to mail-based voting due to COVID-19 does not necessarily make the process less safe*
- Threats in bold are most likely for branch

(c) Natalie M. Scala, 2021

Case Study Takeaways

TOWSON UNIVERSITY | Supply Chain Management

- Consider likelihood of threat
- Attack trees can frame a security problem
- Majority of threat scenarios are tied to insider actions
- Extends into future as mail voting will continue to be used
  - Mail-based voting not as attractive for the adversary
  - Increases voter access
  - Consider U.S. voting policy and proposed legislation
- Greater awareness of where vulnerabilities may exist and relative likelihood
  - Enable officials to apply security measures more effectively and efficiently

(c) Natalie M. Scala, 2021

Managing Insiders

- Proactive training
- Assist with policy compliance
- System design and collaboration in policy design
- Continuous improvement
- Training and awareness to identify and mitigate
- Trusted insider empowered to become part of the solution

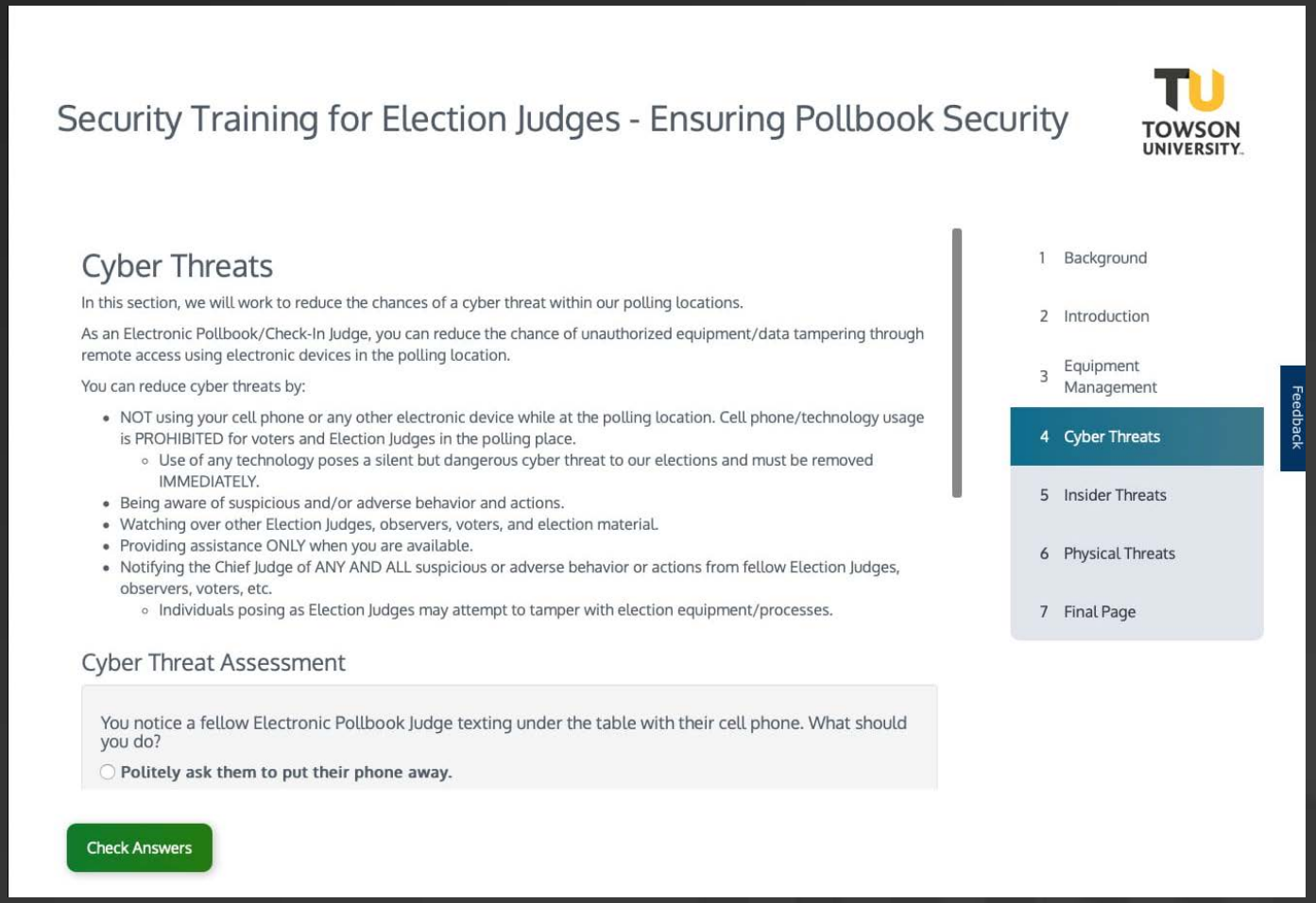
(c) Natalie M. Scala, 2021

Example: Elections Security

TOWSON UNIVERSITY | Supply Chain Management

- Poll worker training
- Sections
  - Background/Introduction
  - Equipment Use
  - Cyber Threats
  - Insider Threats
  - Physical Threats
- Self Assessment Questions
- Certificate of Completion

- Timing: About a week before the election
- Online, at home

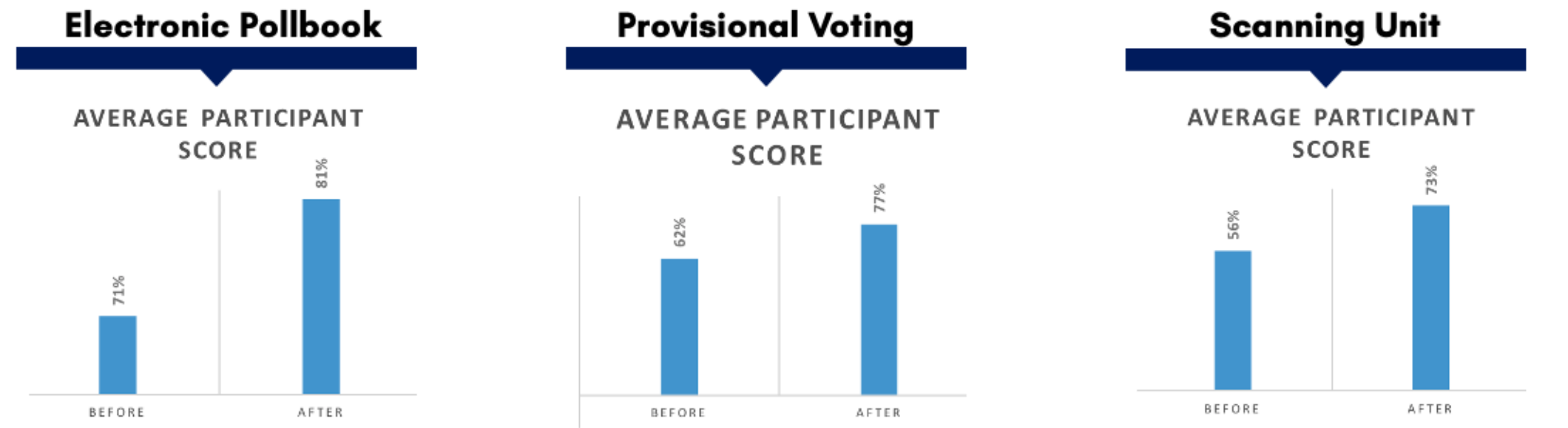


(c) Natalie M. Scala, 2021

Training Works!

TOWSON UNIVERSITY | Supply Chain Management

- Study to examine poll worker knowledge before and after the training
- Quiz scores increased (statistically significant)
  - Awareness of threat
  - Actions to identify, mitigate, and/or eliminate threats
- Usable and accessible



"I am a provisional judge but learned from the questions a lot of information that [Electronic] Pollbook and other judges must perform at the election polls."
– Research Participant

(c) Natalie M. Scala, 2021

Managing Insiders in the Future

TOWSON UNIVERSITY | Supply Chain Management

- Behavior intent
  - Ties to metrics for insider threat
- Security Behaviors Intentions Scale (SeBIS)
  - Egelman and Peer (2015)
  - Egelman, Harbach, Peer (2016)
- Accepted by usable security community to create characterizations
- Choosing passwords, securing devices, updating protocols, proactive awareness
- 16 questions, 5-point Likert scale
- Measure participant intentions and how those intentions may vary
- Does not measure or predict behaviors

(c) Natalie M. Scala, 2021

Models for Behavior Intent

TOWSON UNIVERSITY | Supply Chain Management

- Quantify uncertainty level in personal security intentions
  - Information sharing and patterns
- Identify extent intent connects to pattern of another variable (intention)
  - No presumption of correlation
- Identify infrastructure design actions needed
  - Address poll worker behavior, nature of intent, corresponding risk
  - Low resource environments
- Know your insider!

(c) Natalie M. Scala, 2021

Proactive Modeling Impacts

TOWSON UNIVERSITY | Supply Chain Management

- Artificial intelligence (AI) and machine learning (ML)
- Establish baseline patterns of behavior
- Use prediction capabilities to detect potential anomalies
  - Metrics
- Immediate concerns of profiling
- AI/ML good for quick classification and potential detection
  - Absent of human intervention
  - Human is still part of the process

(c) Natalie M. Scala, 2021

What's the Root Cause Problem?

TOWSON UNIVERSITY | Supply Chain Management

- Build policies and solutions to address
- Misinformation can detract from the root cause problem
- Case study election model
  - Models predicted what happened in U.S. Presidential Election
  - Very little fraud, secure process
- Need to think beyond the discourse and ways we've always solved these problems
- What are the root causes? How much risk willing to take on?
- How do we build cultures of security?

(c) Natalie M. Scala, 2021

Questions and Discussion

TOWSON UNIVERSITY | Supply Chain Management

Dr. Natalie M. Scala

Email: nscala@towson.edu

Web: www.drnataliescala.com

(c) Natalie M. Scala, 2021

References

- ARLIS: Applied Research Laboratory for Intelligence and Security. (2021, March 30). *IRISS event summary #1: State of insider threat and insider risk paradigms.* https://arlis8.umd.edu/iriss-event-summary-1-state-insider-threat-and-insider-risk-paradigms-1
- Black, L., Scala, N. M., Goethals, P. L., & Howard II, J. P. (2018). Values and trends in cybersecurity. *Proceedings of the 2018 Industrial and Systems Engineering Research Conference.* https://tinyurl.com/BlackEtAl2018
- Dehlinger, J., Harrison, S., & Scala, N. M. (2021). Pollworker security: Assessment and design of usability and performance. *Proceedings of the 2021 IISE Annual Conference.* https://tinyurl.com/hvwde2ep
- Department of Homeland Security. (2020, July 14). *Election security.* https://www.dhs.gov/topic/election-security
- Du, S., & Zhu, H. (2013). *Security assessment in vehicular networks.* Springer.
- Egelman, S., Harbach, M., & Peer, E. (2016). Behavior ever follows intention? A validation of the Security Behavior Intentions Scale (SeBIS). *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems,* 5257-5261.

References

- Egelman, S. & Peer, E. (2015). Scaling the security wall: Developing a Security Behavior Intentions Scale (SeBIS). *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems,* 2873-2882.
- Horwitz, S., Nakashima, E., & Gold, M. (2017). DHS tells states about Russian hacking in 2016 election. *The Washington Post.* https://tinyurl.com/HorwitzEtAl
- Locraft, H., Gajendiran, P., Price, M., Scala, N. M., & Goethals, P. L. (2019). Sources of risk in elections security. *Proceedings of the 2019 IISE Annual Conference.* https://tinyurl.com/LocraftEtAl2019
- Mueller III, R. S. (2019). Former Special Counsel Robert S. Mueller, III on the Investigation into Russian Interference in the 2016 Presidential Election. *U.S. House of Representatives Committee Repository,* https://docs.house.gov/meetings/IG/IG00/20190724/109808/HHRG-116-IG00-Transcript-20190724.pdf
- Price, M., Scala, N. M., & Goethals, P. L. (2019). Protecting Maryland's voting processes. *Baltimore Business Review: A Maryland Journal*. https://www.cfasociety.org/baltimore/Documents/BBR_2019%20Final.pdf#page=38
- Root, D., Kennedy, L., Sozan, M., & Parshall, J. (2018). Election security in all 50 states. https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/

(c) Natalie M. Scala, 2021

References

- Sanger, D. & Edmonson, C. (2019, July 25). Russia targeted election systems in all 50 states, report finds. *The New York Times.* https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html
- Scala, N. M., Dehlinger, J., Black, L., Harrison, S., Delgado Licona, K., & Ieromonahos, A. (2020). Empowering election judges to secure our elections*. Baltimore Business Review: A Maryland Journal,* 8-20.
- Scala, N. M. & Goethals, P. L. (2020). A model for and inventory of cybersecurity values: Metrics and best practices. In N. M. Scala and J. P. Howard II (Eds.), *Handbook of Military and Defense Operations Research* (pp. 305-330). CRC Press.
- Scala, N. M., Goethals, P. L., Dehlinger, J., Mezgebe, Y., Jilcha, B., & Bloomquist, I. (2021). Evaluating mail-in security for electoral processes using attack trees. Under review.
- United States Election Assistance Commission Advisory Board. (2009). *Election operations assessment: Threat trees and matrices and threat instance risk analyzer (TIRA).* https://www.eac.gov/assets/1/28/Election_Operations_Assessment_Threat_Trees_and_Matrices_and_Threat_Instance_Risk_Analyzer_(TIRA).pdf
- United States Election Assistance Commission Advisory Board. (2018). *Help America Vote Act.* https://www.eac.gov/about/help-america-vote-act/

(c) Natalie M. Scala, 2021