Experimental aspects of investigating the failures and shortcomings of security countermeasures

Md Rayhanur Rahman, Brandon Wroblewski, Mahzabin Tamanna, Imranur Rahman, Andrew Anufryienak, Laurie Williams

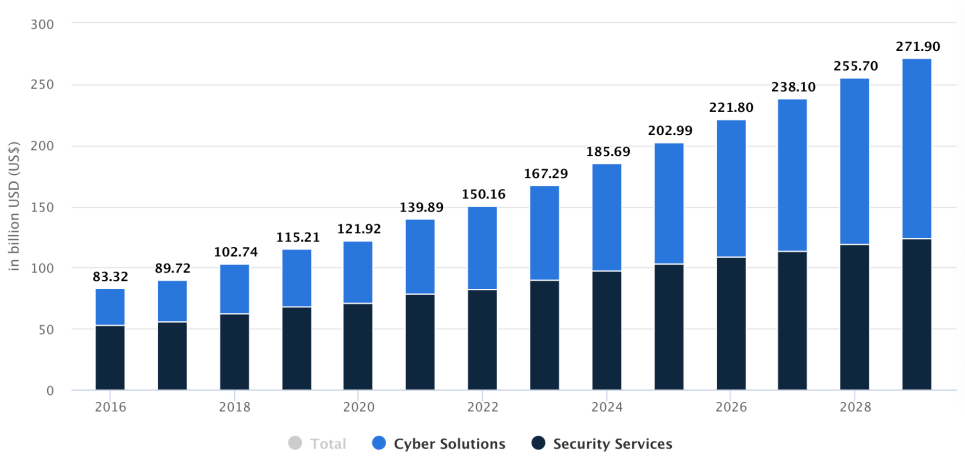
NC State University

Cost of securing organizations

$271B spent worldwide

60% up over last 5 years

$10.5T direct and indirect cost



Statista

But we are seeing more attacks



49M customer data leaked



400GB patient data stolen



Ransomware encrypts company emails, payroll and other documents

Practitioners Perspective on Security Controls

36%

controls are working as intended

42%

understand control failures and track their improvement

82%

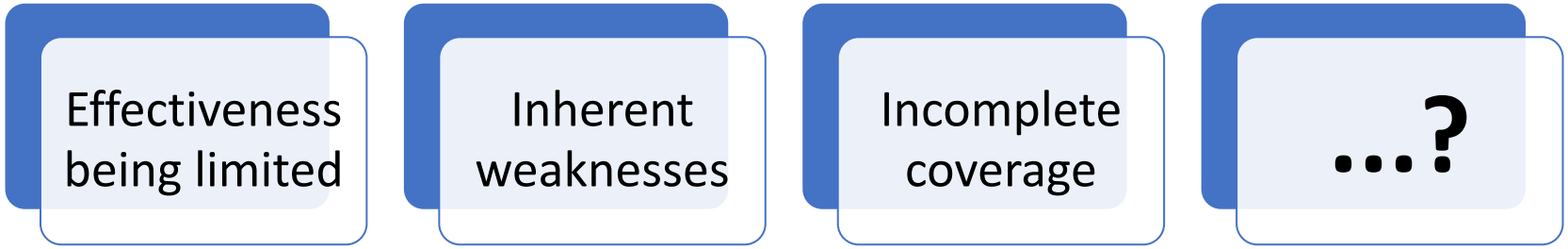
surprised that an attack happened except controls were enforced

60%

lacks in measuring the effectiveness of controls

Panaseer 2022 Security Leaders Peer Report

We hypothesize that security control implementation is challenging



A taxonomy of such challenges would benefit practitioners, and we can leverage Large Language Models to construct such taxonomy

Goal and RQs

The goal of this study is to aid security practitioners in defending against cyberattacks by constructing a taxonomy of challenges in security control implementation

RQ1: How can we leverage LLMs to construct a taxonomy of challenges in security control implementations?
RQ2: What prevalent challenges in security control implementation are responsible for cyberattacks?

Overall Findings



Taxonomy

Eight categories of challenges

73 challenges in total



Prevalent Challenges

Human resource

False Positives

Compatibility

Talk: Towards a Taxonomy of Challenges in Security Control Implementation
Wednesday 11:30 (Generative AI (for) Security)

Research Design Aspects



Traditional User Survey?



Systematic Academic and Grey Literature Search?

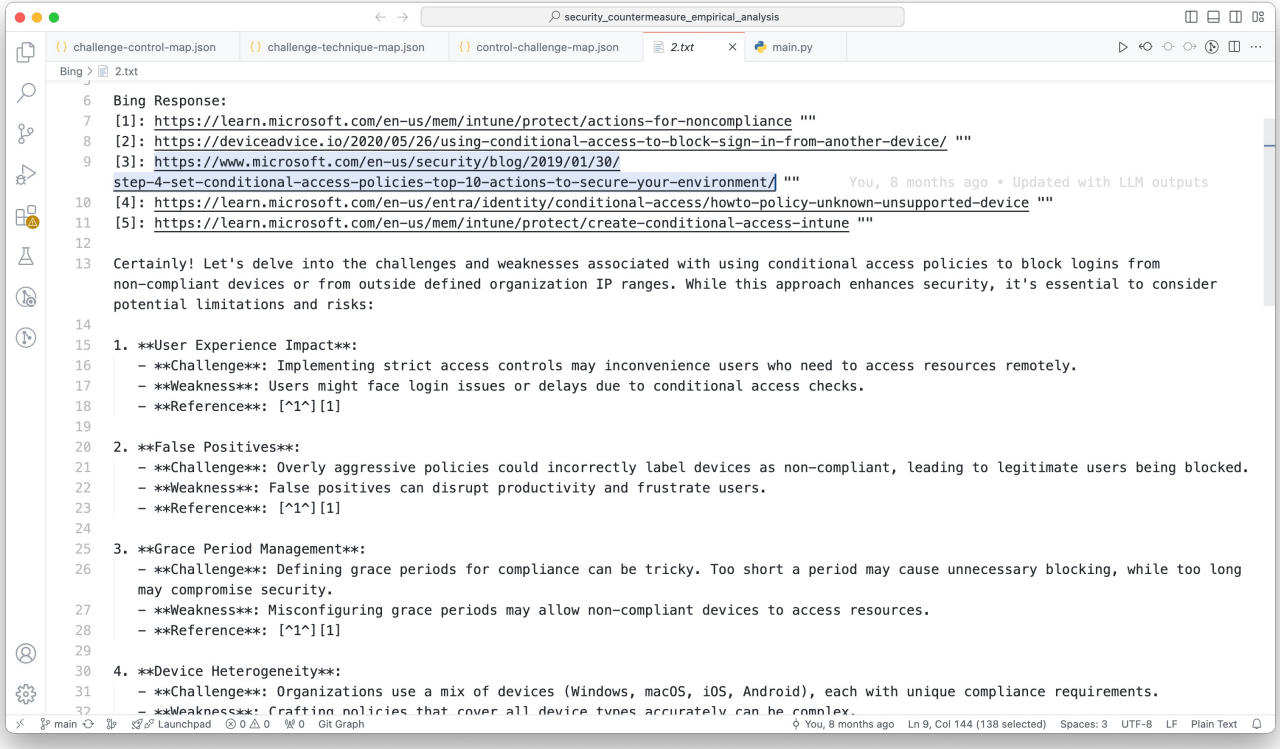


Take advantage of LLMs

Prompt Engineering

You are Copilot, a large language model by Bing. You are a helpful assistant. Imagine that you are a cybersecurity expert. I will give you a security control. You will generate a list of challenges, and weaknesses for the control. For each item in the generated list, you will provide references. Security control: Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges

Response


security_countermeasure_empirical_analysis
challenge-control-map.json
challenge-technique-map.json
control-challenge-map.json
2.txt
main.py
Bing > 2.txt
Bing Response:
[1]: https://learn.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance ""
[2]: https://deviceadvice.io/2020/05/26/using-conditional-access-to-block-sign-in-from-another-device/ ""
[3]: https://www.microsoft.com/en-us/security/blog/2019/01/30/step-4-set-conditional-access-policies-top-10-actions-to-secure-your-environment/ ""
You, 8 months ago • Updated with LLM outputs
[4]: https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-policy-unknown-unsupported-device ""
[5]: https://learn.microsoft.com/en-us/mem/intune/protect/create-conditional-access-intune ""
Certainly! Let's delve into the challenges and weaknesses associated with using conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. While this approach enhances security, it's essential to consider potential limitations and risks:
1. **User Experience Impact**:
- **Challenge**: Implementing strict access controls may inconvenience users who need to access resources remotely.
- **Weakness**: Users might face login issues or delays due to conditional access checks.
- **Reference**: [^1^][1]
2. **False Positives**:
- **Challenge**: Overly aggressive policies could incorrectly label devices as non-compliant, leading to legitimate users being blocked.
- **Weakness**: False positives can disrupt productivity and frustrate users.
- **Reference**: [^1^][1]
3. **Grace Period Management**:
- **Challenge**: Defining grace periods for compliance can be tricky. Too short a period may cause unnecessary blocking, while too long may compromise security.
- **Weakness**: Misconfiguring grace periods may allow non-compliant devices to access resources.
- **Reference**: [^1^][1]
4. **Device Heterogeneity**:
- **Challenge**: Organizations use a mix of devices (Windows, macOS, iOS, Android), each with unique compliance requirements.
main
Launchpad
Git Graph
You, 8 months ago
Ln 9, Col 144 (138 selected)
Spaces: 3
UTF-8
LF
Plain Text

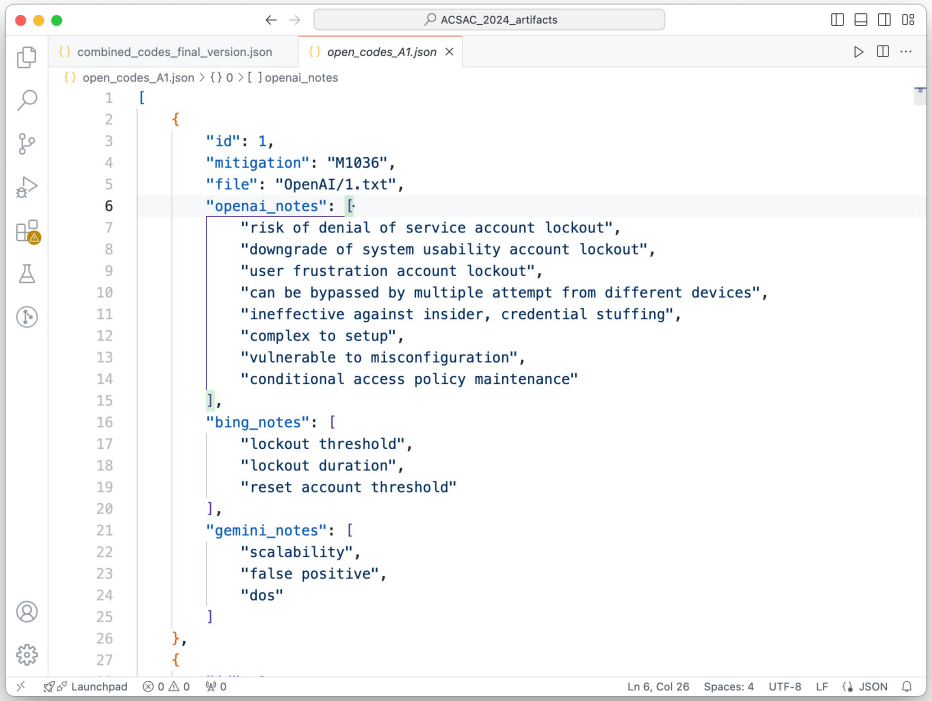
Filtering the responses

- Inclusion and exclusion criteria
  - challenges and limitations directly related to the control
  - challenges and limitations that are relevant to modern technology and tools
  - limitation that can open up attack vectors
  - generic implementation faults such as human error or misconfiguration;
  - hallucinated results that are not relevant to the controls or factually incorrect;
  - error messages;
  - limitations that are not inherently related to the specific controls; and
  - limitations related to bypassing mechanisms by adversaries

Subjective Analysis – First Round

- Open Coding & Inductive Coding
- Coding Granularity
  - *Long and strong passwords are inconvenient, which leads to writing down a password*
- Different codes for the same issue
  - *Patches can introduce new vulnerabilities*
  - *Vulnerable patches*

Intermediate Output – First Round Coding



Subjective Analysis – Second Round



Reflexive Thematic Analysis

Resolving granularity and inconsistent coding issue

Combining different perspective

Theme and sub-themes

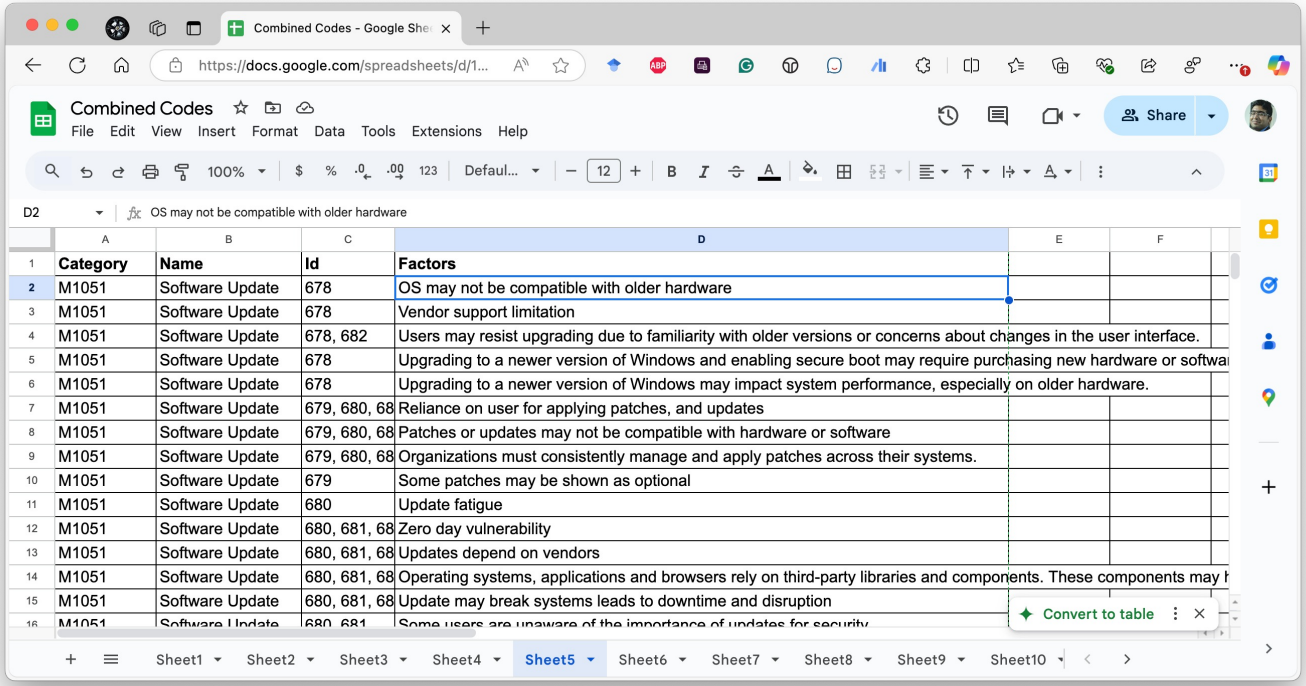


Validation

Inter-rater agreement is time consuming

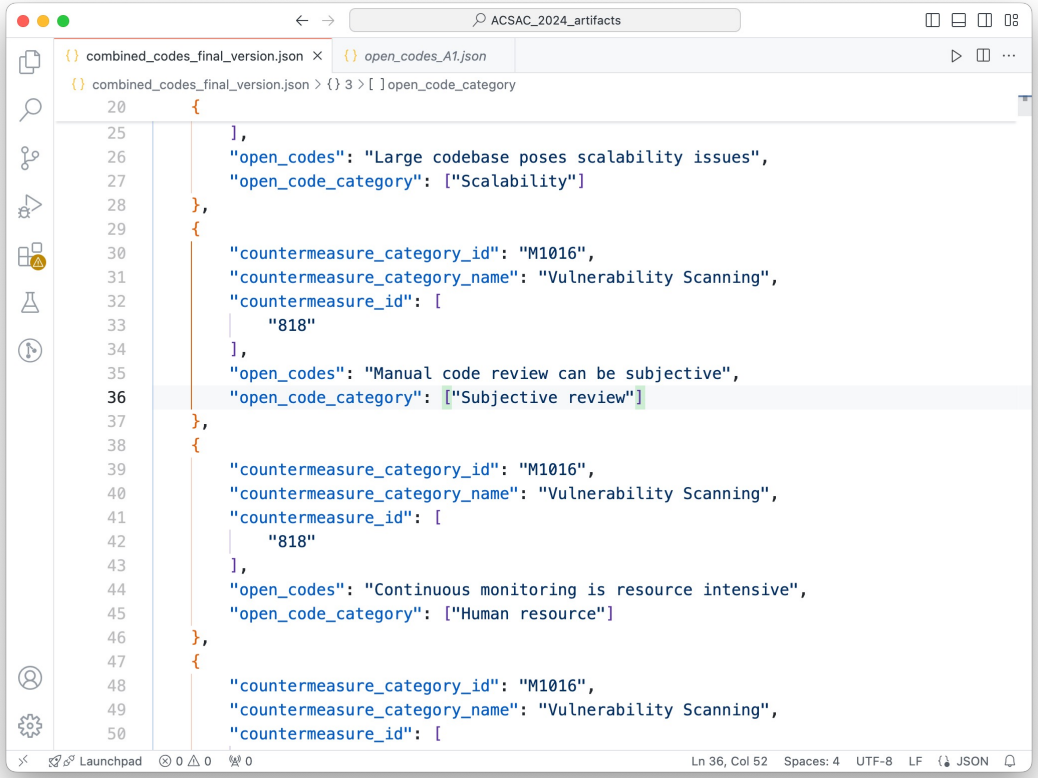
Focus on agreement through discussion

Combined Codes after Thematic Analysis



	A	B	C	D	E	F
1	**Category**	**Name**	**Id**	**Factors**		
2	M1051	Software Update	678	OS may not be compatible with older hardware		
3	M1051	Software Update	678	Vendor support limitation		
4	M1051	Software Update	678, 682	Users may resist upgrading due to familiarity with older versions or concerns about changes in the user interface.		
5	M1051	Software Update	678	Upgrading to a newer version of Windows and enabling secure boot may require purchasing new hardware or softwa		
6	M1051	Software Update	678	Upgrading to a newer version of Windows may impact system performance, especially on older hardware.		
7	M1051	Software Update	679, 680, 68	Reliance on user for applying patches, and updates		
8	M1051	Software Update	679, 680, 68	Patches or updates may not be compatible with hardware or software		
9	M1051	Software Update	679, 680, 68	Organizations must consistently manage and apply patches across their systems.		
10	M1051	Software Update	679	Some patches may be shown as optional		
11	M1051	Software Update	680	Update fatigue		
12	M1051	Software Update	680, 681, 68	Zero day vulnerability		
13	M1051	Software Update	680, 681, 68	Updates depend on vendors		
14	M1051	Software Update	680, 681, 68	Operating systems, applications and browsers rely on third-party libraries and components. These components may h		
15	M1051	Software Update	680, 681, 68	Update may break systems leads to downtime and disruption		
16	M1051	Software Update	680, 681	Some users are unaware of the importance of updates for security		

Final Set of Codes



Dataset Used for RQ1



Security controls – MITRE ATT&CK



NIST SP800-53 / CIS Top 20 are too abstract

Example – Controls for Phishing

Mitigations

ID	Mitigation	Description
M1049	Antivirus/Antimalware	Anti-virus can automatically quarantine suspicious files.
M1047	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.
M1031	Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity.
M1021	Restrict Web-Based Content	Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.
M1054	Software Configuration	Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.[17][18]
M1017	User Training	Users can be trained to identify social engineering techniques and phishing emails.

RQ1 Methodology - Further Discussion

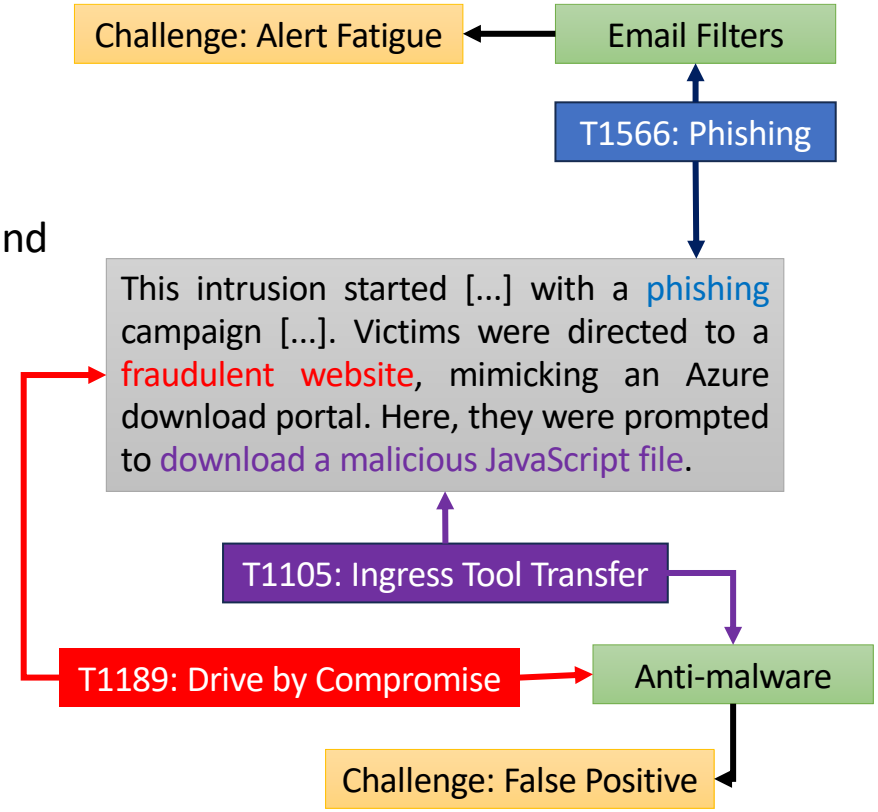
- Prior methodology
  - Codifying challenges directly from reading the control statements
  - Based on the coders' subjective judgement and domain knowledge
  - Abandoned
    - Time consuming
    - No standard methodology
    - Difference between two raters' identified codes are widely varied
- Potential Improvements
  - External Validation
  - Systematic Search
  - Discussing with practitioners
  - Findings could be domain-dependent

How can we Identify **Prevalent** Challenges?

- Availability?
- Traceability?
- Generalizability?

Methodology for RQ2

- Case Study – as generalization is infeasible
- Data source – CTI reports
  - CTI Reports mentions attack techniques
- Hypothetical mapping between techniques and challenges
  - Techniques have mitigating controls
  - Controls have associated challenges
- Dataset
  - 30 MITRE ATT&CK Campaigns
  - 667 CTI Reports
  - 94 technique sequence datasets
- Analysis
  - Identify prevalent techniques
  - identify prevalent controls
  - Identify prevalent challenges



Further Discussion

- More speculative - no validation
- Findings could’ve been more granular
- Generalizability may be limiting
  - Specific implementation of controls
  - Expertise and skills of practitioners
  - Unknown challenges

Meta-Discussion

- Did you use experimentation artifacts borrowed from the community? No
- Did you attempt to replicate or reproduce results of earlier research as part of your work? No
- What can be learned from your methodology and your experience using your methodology?
- What did you try that did not succeed before getting to the results you presented?
- Did you produce any intermediate results including possible unsuccessful tests or experiments? Yes

Future Research Directions

- Why do security controls fail and what are the underlying factors
- Which stream of security investment as a priority – human vs technology?
- How effective is the security controls?
  - Metrics?
  - Methods?
  - Maturity?
- What can be done to implement “shift left” approach everywhere?
- How can we design security control targeting social, psychological, and other human factors?

Contact me: mdrayhanur.rahman@ua.edu
Web: https://rayhanur-rahman.github.io/