California State University
Northridge

SRA 2020
Risk Science for Sustainability

Enhancing Cybersecurity: Systematic Investigation of Insider Threats Utilizing the AcciMap Framework

Cyber Safe

Shorouk Bekir and Maryam Tabibzadeh

December 15, 2020

AGENDA

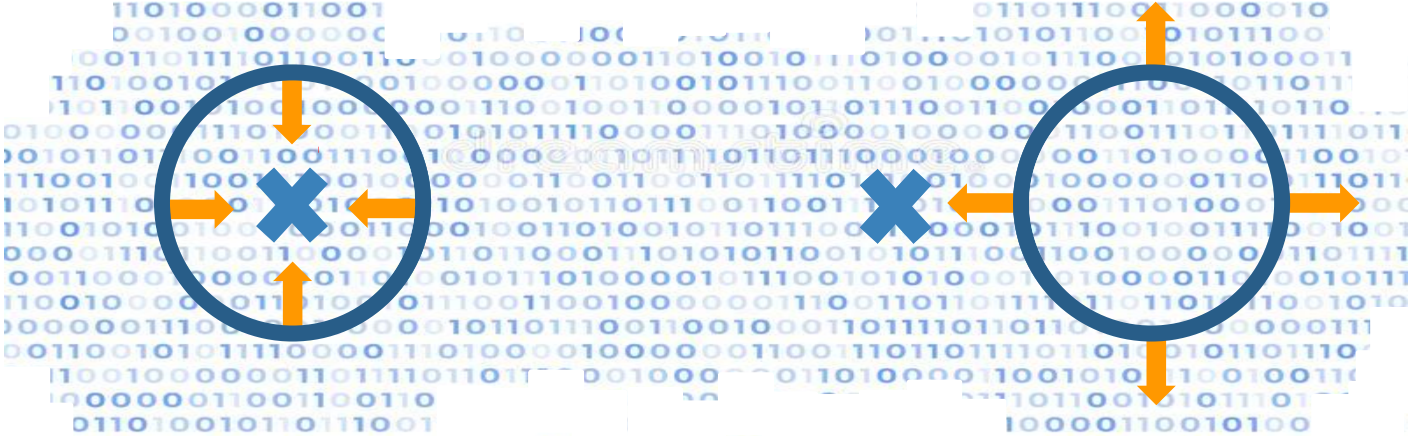
- Introduction
- Methodology
- AcciMap Development & Analysis
- Recommendations
- Conclusion

1

INTRODUCTION

The Insider and Outsider Threat

INTRODUCTION



Insider Threat

Outsider Threat

STATISTICS

From 2018 up-to-date

2018...2019...
2020?

The overall cost of insider threats has increased from $8.76M to $11.45M **31% Increase**

The number of incidents has increased from 3,200 to 4,700 incidents **47% Increase**

The average cost of an incident investigation increased from $75,215 to $103,798 **38% Increase**

STATISTICS

5% NON EXSISTENT

of the organizations have no mature security capabilities that monitor insider threats

24% REACTIVE

of the organizations have no prediction programs for insider threats

48% PROACTIVE

of the organizations monitor employees with potential malicious behaviors

16% PREDICTIVE

of the organizations establish appropriate levels of monitoring to all employees

7% OPTIMIZED

of the organizations have a mature view of insider threat risk

2

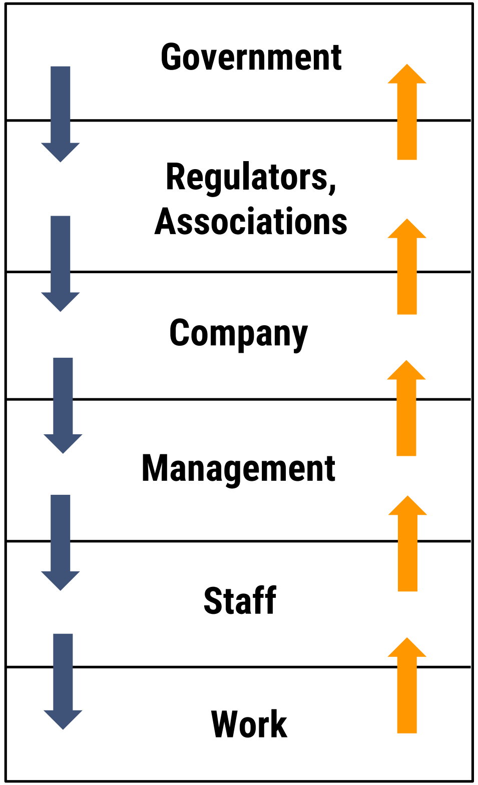
METHODOLOGY

Rasmussen's Risk Management Framework and The AcciMap

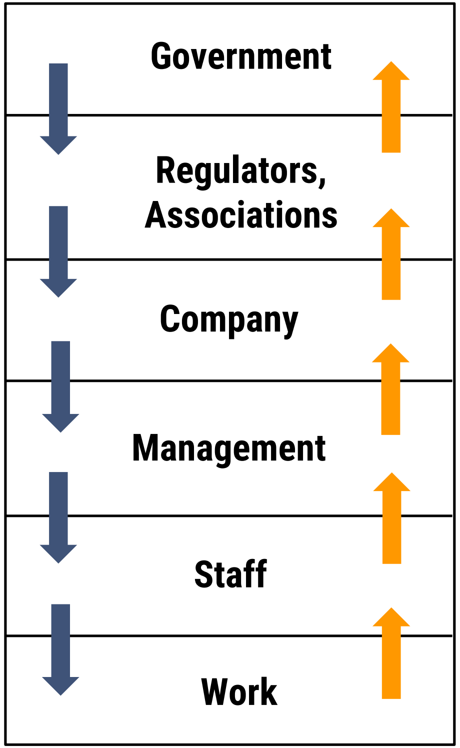
RISK MANAGEMENT FRAMEWORK

- The foundation of the proposed methodology is based on a dynamic risk management framework originally developed by Rasmussen.

- The framework is underpinned by the idea that various levels can interact with one another shaping culture, behavior, safety and possibly threats.



RASMUSSEN’S ACCIMAP



Government

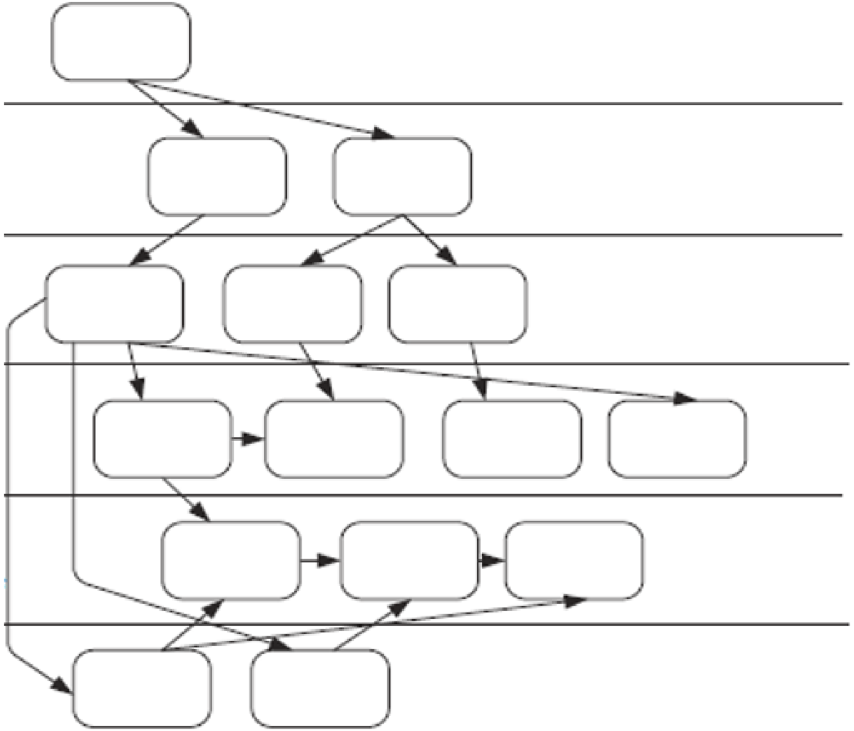
Regulators, Associations

Company

Management

Staff

Work



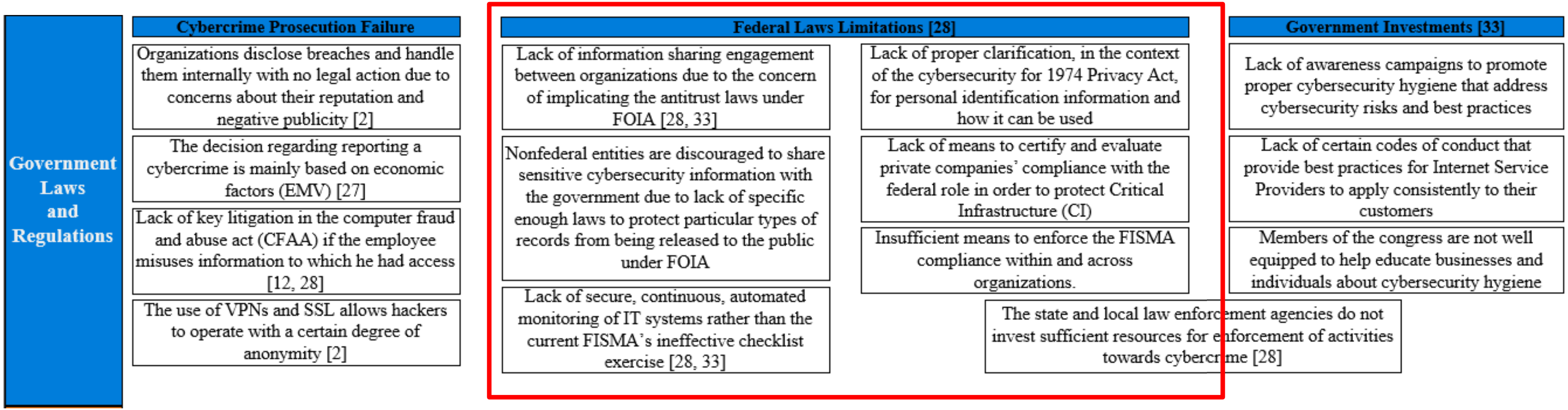
□ = Failures, decisions, actions, etc.

3

ACCIMAP ANALYSIS

Contributing Causes, Findings and Observations

DEVELOPED ACCIMAP TO INVESTIGATE INSIDER THREATS



Government Laws and Regulations

Cybercrime Prosecution Failure

- Organizations disclose breaches and handle them internally with no legal action due to concerns about their reputation and negative publicity [2]
- The decision regarding reporting a cybercrime is mainly based on economic factors (EMV) [27]
- Lack of key litigation in the computer fraud and abuse act (CFAA) if the employee misuses information to which he had access [12, 28]
- The use of VPNs and SSL allows hackers to operate with a certain degree of anonymity [2]

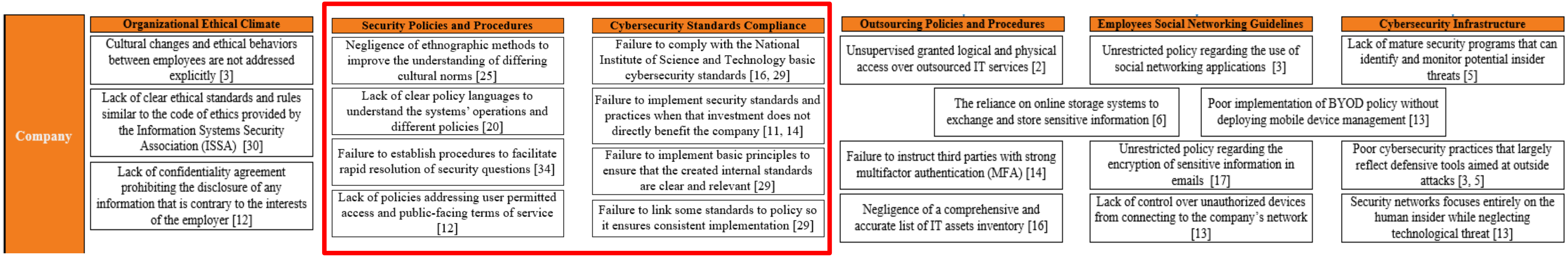
Federal Laws Limitations [28]

- Lack of information sharing engagement between organizations due to the concern of implicating the antitrust laws under FOIA [28, 33]
- Nonfederal entities are discouraged to share sensitive cybersecurity information with the government due to lack of specific enough laws to protect particular types of records from being released to the public under FOIA
- Lack of secure, continuous, automated monitoring of IT systems rather than the current FISMA's ineffective checklist exercise [28, 33]
- Lack of proper clarification, in the context of the cybersecurity for 1974 Privacy Act, for personal identification information and how it can be used
- Lack of means to certify and evaluate private companies' compliance with the federal role in order to protect Critical Infrastructure (CI)
- Insufficient means to enforce the FISMA compliance within and across organizations.

Government Investments [33]

- Lack of awareness campaigns to promote proper cybersecurity hygiene that address cybersecurity risks and best practices
- Lack of certain codes of conduct that provide best practices for Internet Service Providers to apply consistently to their customers
- Members of the congress are not well equipped to help educate businesses and individuals about cybersecurity hygiene
- The state and local law enforcement agencies do not invest sufficient resources for enforcement of activities towards cybercrime [28]

DEVELOPED ACCIMAP TO INVESTIGATE INSIDER THREATS-CONT'D



Company

Organizational Ethical Climate

Cultural changes and ethical behaviors between employees are not addressed explicitly [3]

Lack of clear ethical standards and rules similar to the code of ethics provided by the Information Systems Security Association (ISSA) [30]

Lack of confidentiality agreement prohibiting the disclosure of any information that is contrary to the interests of the employer [12]

Security Policies and Procedures

Negligence of ethnographic methods to improve the understanding of differing cultural norms [25]

Lack of clear policy languages to understand the systems' operations and different policies [20]

Failure to establish procedures to facilitate rapid resolution of security questions [34]

Lack of policies addressing user permitted access and public-facing terms of service [12]

Cybersecurity Standards Compliance

Failure to comply with the National Institute of Science and Technology basic cybersecurity standards [16, 29]

Failure to implement security standards and practices when that investment does not directly benefit the company [11, 14]

Failure to implement basic principles to ensure that the created internal standards are clear and relevant [29]

Failure to link some standards to policy so it ensures consistent implementation [29]

Outsourcing Policies and Procedures

Unsupervised granted logical and physical access over outsourced IT services [2]

The reliance on online storage systems to exchange and store sensitive information [6]

Failure to instruct third parties with strong multifactor authentication (MFA) [14]

Negligence of a comprehensive and accurate list of IT assets inventory [16]

Employees Social Networking Guidelines

Unrestricted policy regarding the use of social networking applications [3]

Poor implementation of BYOD policy without deploying mobile device management [13]

Unrestricted policy regarding the encryption of sensitive information in emails [17]

Lack of control over unauthorized devices from connecting to the company's network [13]

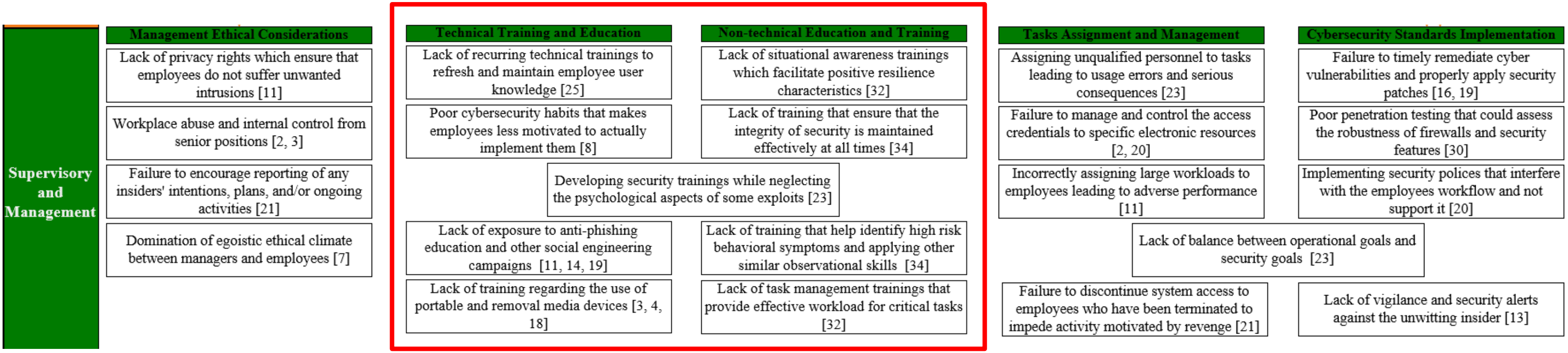
Cybersecurity Infrastructure

Lack of mature security programs that can identify and monitor potential insider threats [5]

Poor cybersecurity practices that largely reflect defensive tools aimed at outside attacks [3, 5]

Security networks focuses entirely on the human insider while neglecting technological threat [13]

DEVELOPED ACCIMAP TO INVESTIGATE INSIDER THREATS-CONT'D



Supervisory and Management

Management Ethical Considerations

Lack of privacy rights which ensure that employees do not suffer unwanted intrusions [11]

Workplace abuse and internal control from senior positions [2, 3]

Failure to encourage reporting of any insiders' intentions, plans, and/or ongoing activities [21]

Domination of egoistic ethical climate between managers and employees [7]

Technical Training and Education

Lack of recurring technical trainings to refresh and maintain employee user knowledge [25]

Poor cybersecurity habits that makes employees less motivated to actually implement them [8]

Lack of exposure to anti-phishing education and other social engineering campaigns [11, 14, 19]

Lack of training regarding the use of portable and removal media devices [3, 4, 18]

Non-technical Education and Training

Lack of situational awareness trainings which facilitate positive resilience characteristics [32]

Lack of training that ensure that the integrity of security is maintained effectively at all times [34]

Lack of training that help identify high risk behavioral symptoms and applying other similar observational skills [34]

Lack of task management trainings that provide effective workload for critical tasks [32]

Developing security trainings while neglecting the psychological aspects of some exploits [23]

Tasks Assignment and Management

Assigning unqualified personnel to tasks leading to usage errors and serious consequences [23]

Failure to manage and control the access credentials to specific electronic resources [2, 20]

Incorrectly assigning large workloads to employees leading to adverse performance [11]

Failure to discontinue system access to employees who have been terminated to impede activity motivated by revenge [21]

Cybersecurity Standards Implementation

Failure to timely remediate cyber vulnerabilities and properly apply security patches [16, 19]

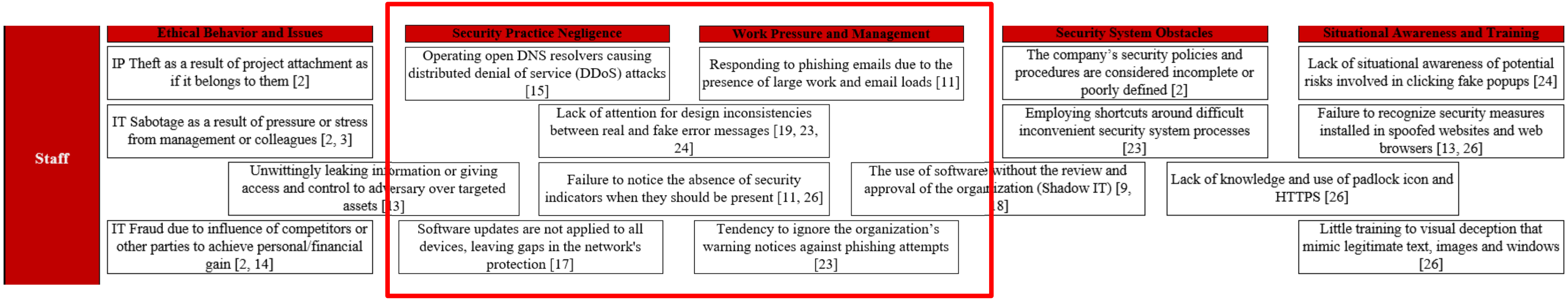
Poor penetration testing that could assess the robustness of firewalls and security features [30]

Implementing security polices that interfere with the employees workflow and not support it [20]

Lack of vigilance and security alerts against the unwitting insider [13]

Lack of balance between operational goals and security goals [23]

DEVELOPED ACCIMAP TO INVESTIGATE INSIDER THREATS-CONT'D



Staff

Ethical Behavior and Issues

Security Practice Negligence

Work Pressure and Management

Security System Obstacles

Situational Awareness and Training

IP Theft as a result of project attachment as if it belongs to them [2]

Operating open DNS resolvers causing distributed denial of service (DDoS) attacks [15]

Responding to phishing emails due to the presence of large work and email loads [11]

The company's security policies and procedures are considered incomplete or poorly defined [2]

Lack of situational awareness of potential risks involved in clicking fake popups [24]

IT Sabotage as a result of pressure or stress from management or colleagues [2, 3]

Lack of attention for design inconsistencies between real and fake error messages [19, 23, 24]

Employing shortcuts around difficult inconvenient security system processes [23]

Failure to recognize security measures installed in spoofed websites and web browsers [13, 26]

Unwittingly leaking information or giving access and control to adversary over targeted assets [13]

Failure to notice the absence of security indicators when they should be present [11, 26]

The use of software without the review and approval of the organization (Shadow IT) [9, 18]

Lack of knowledge and use of padlock icon and HTTPS [26]

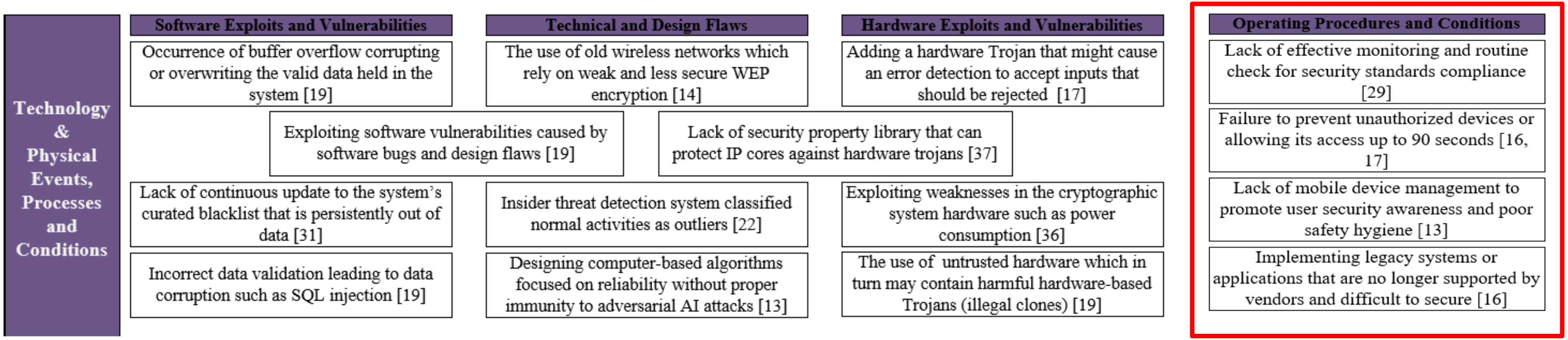
IT Fraud due to influence of competitors or other parties to achieve personal/financial gain [2, 14]

Software updates are not applied to all devices, leaving gaps in the network's protection [17]

Tendency to ignore the organization's warning notices against phishing attempts [23]

Little training to visual deception that mimic legitimate text, images and windows [26]

DEVELOPED ACCIMAP TO INVESTIGATE INSIDER THREATS-CONT'D



Technology & Physical Events, Processes and Conditions

Software Exploits and Vulnerabilities

Occurrence of buffer overflow corrupting or overwriting the valid data held in the system [19]

Lack of continuous update to the system's curated blacklist that is persistently out of data [31]

Incorrect data validation leading to data corruption such as SQL injection [19]

Exploiting software vulnerabilities caused by software bugs and design flaws [19]

Technical and Design Flaws

The use of old wireless networks which rely on weak and less secure WEP encryption [14]

Insider threat detection system classified normal activities as outliers [22]

Designing computer-based algorithms focused on reliability without proper immunity to adversarial AI attacks [13]

Lack of security property library that can protect IP cores against hardware trojans [37]

Hardware Exploits and Vulnerabilities

Adding a hardware Trojan that might cause an error detection to accept inputs that should be rejected [17]

Exploiting weaknesses in the cryptographic system hardware such as power consumption [36]

The use of untrusted hardware which in turn may contain harmful hardware-based Trojans (illegal clones) [19]

Operating Procedures and Conditions

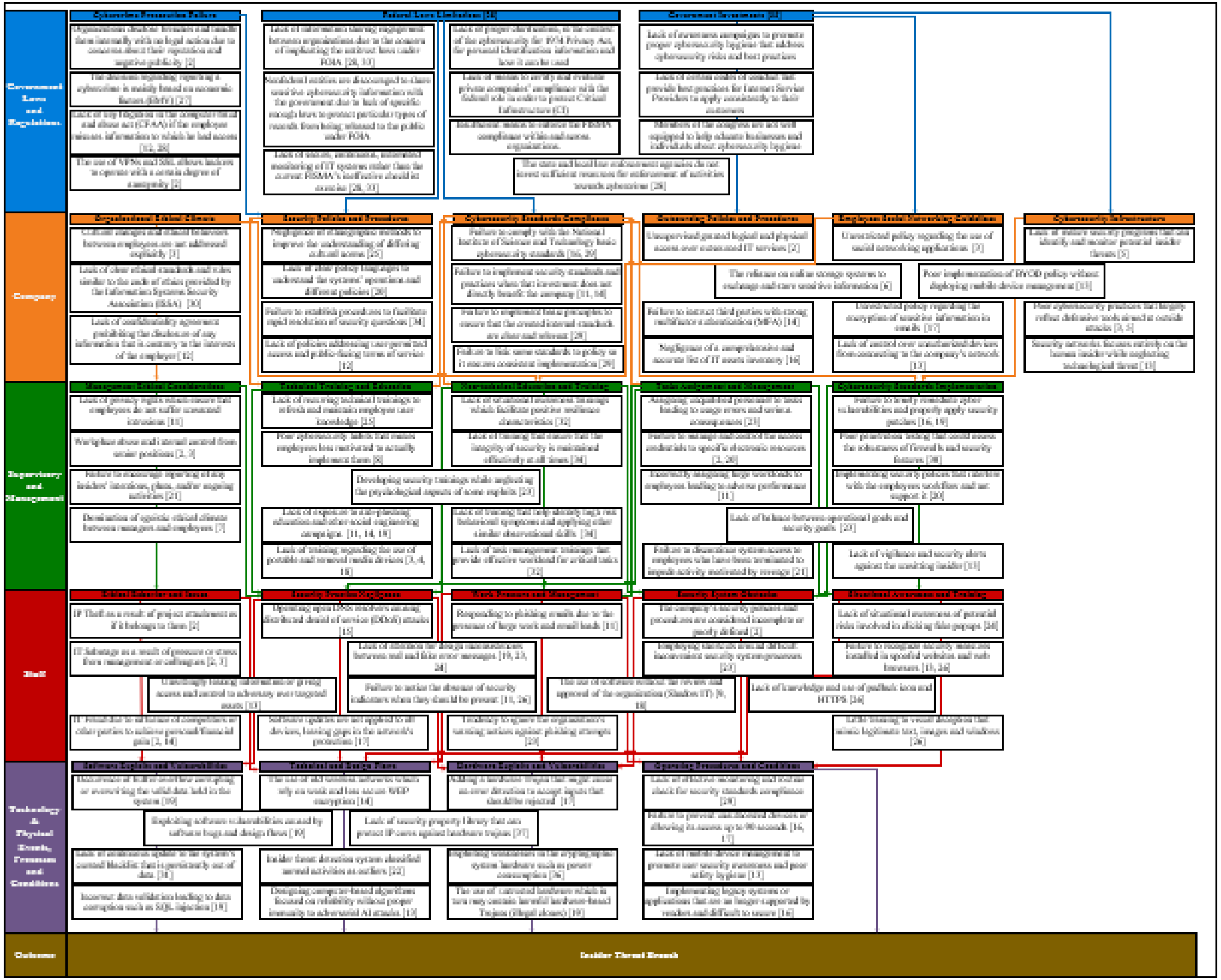
Lack of effective monitoring and routine check for security standards compliance [29]

Failure to prevent unauthorized devices or allowing its access up to 90 seconds [16, 17]

Lack of mobile device management to promote user security awareness and poor safety hygiene [13]

Implementing legacy systems or applications that are no longer supported by vendors and difficult to secure [16]

DEVELOPED ACCIMAP TO INVESTIGATE INSIDER THREATS



Government Laws and Regulations

Cybercrime Prosecution Failure
- Organizations disallow breaches and handle them internally with no legal action due to concerns about their reputation and negative publicity [2]
- The decision regarding reporting a cybercrime is mainly based on economic factors (ROI) [27]
- Lack of any litigation on the computer fraud and abuse act (CFAA) if the employee misuses information to which he had access [12, 28]
- The use of VPNs and SSL allows hackers to operate with a certain degree of anonymity [2]

Federal Laws Limitations [28]
- Lack of information sharing engagement between organizations due to the concern of implicating the antitrust laws under FOIA [28, 33]
- Nonfederal entities are discouraged to share sensitive cybersecurity information with the government due to lack of specific enough laws to protect particular types of records from being released to the public under FOIA
- Lack of secure, continuous, automated monitoring of IT systems rather than the current FISMA's ineffective checklist exercise [28, 33]
- Lack of proper clarifications, in the context of the cybersecurity for FOIA Privacy Act, for personal identification information and how it can be used
- Lack of means to certify and evaluate private companies' compliance with the federal role in order to protect Critical Infrastructure (CI)
- Insufficient means to enforce the FISMA compliance within and across organizations.
- The state and local law enforcement agencies do not invest sufficient resources for enforcement of activities towards cybercrime [28]

Government Investments [22]
- Lack of awareness campaigns to promote proper cybersecurity hygiene that address cybersecurity risks and best practices
- Lack of certain codes of conduct that provide best practices for Internet Service Providers to apply consistently to their customers
- Members of the congress are not well equipped to help educate businesses and individuals about cybersecurity hygiene

Company

Organizational Ethical Climate
- Cultural changes and ethical behaviors between employees are not addressed explicitly [3]
- Lack of clear ethical standards and rules similar to the code of ethics provided by the Information Systems Security Association (ISSA) [30]
- Lack of confidentiality agreement prohibiting the disclosure of any information that is contrary to the interests of the employer [12]

Security Policies and Procedures
- Negligence of ethnographic methods to improve the understanding of differing cultural norms [25]
- Lack of clear policy languages to understand the systems' operations and different policies [20]
- Failure to establish procedures to facilitate rapid resolution of security questions [34]
- Lack of policies addressing user-permitted access and public-facing terms of service [12]

Cybersecurity Standards Compliance
- Failure to comply with the National Institute of Standards and Technology basic cybersecurity standards [16, 29]
- Failure to implement security standards and practices when their investment does not directly benefit the company [11, 16]
- Failure to implement basic principles to ensure that the created internal standards are clear and relevant [29]
- Failure to link same standards to policy so it ensures consistent implementation [29]

Outsourcing Policies and Procedures
- Unsupervised granted logical and physical access over outsourced IT services [2]
- The reliance on online storage systems to exchange and store sensitive information [6]
- Failure to instruct third parties with strong multifactor authentication (MFA) [14]
- Negligence of a comprehensive and accurate list of IT assets inventory [16]

Employee Social Networking Guidelines
- Unrestricted policy regarding the use of social networking applications [3]
- Poor implementation of BYOD policy without deploying mobile device management [13]
- Unrestricted policy regarding the encryption of sensitive information in emails [17]
- Lack of control over unauthorized devices from connecting to the company's network [13]

Cybersecurity Infrastructure
- Lack of mature security programs that can identify and monitor potential insider threats [5]
- Poor cybersecurity practices that largely reflect defensive tools aimed at outside attacks [3, 5]
- Security networks focuses entirely on the human insider while neglecting technological threat [13]

Supervisory and Management

Management Ethical Considerations
- Lack of privacy rights which ensure that employees do not suffer unwanted intrusions [11]
- Workplace abuse and internal control from senior positions [2, 3]
- Failure to encourage reporting of any insiders' intentions, plans, and/or ongoing activities [21]
- Domination of egoistic ethical climate between managers and employees [7]

Technical Training and Education
- Lack of recurring technical trainings to refresh and maintain employees' user knowledge [25]
- Poor cybersecurity habits that makes employees less motivated to actually implement them [8]
- Developing security trainings while neglecting the psychological aspects of some exploits [23]
- Lack of exposure to a role-playing situation and other social engineering campaigns [11, 14, 15]
- Lack of training regarding the use of portable and removal media devices [3, 4, 18]

Non-technical Education and Training
- Lack of situational awareness trainings which facilitate positive resilience characteristics [32]
- Lack of training that ensure that the integrity of security is maintained effectively at all times [34]
- Lack of training that help identify high risk behavioral symptoms and applying other similar observational skills [34]
- Lack of task management trainings that provide effective workload for critical tasks [32]

Tasks Assignment and Management
- Assigning unqualified personnel to tasks leading to usage errors and serious consequences [23]
- Failure to manage and control the access credentials to specific electronic resources [2, 20]
- Incorrectly assigning large workloads to employees leading to adverse performance [11]
- Lack of balance between operational goals and security goals [23]
- Failure to discontinue system access to employees who have been terminated to impede activity motivated by revenge [21]

Cybersecurity Standards Implementation
- Failure to timely remediate cyber vulnerabilities and properly apply security patches [16, 19]
- Poor penetration testing that could assess the robustness of firewalls and security features [38]
- Implementing security policies that interfere with the employees workflow and not support it [20]
- Lack of vigilance and security alerts against the unwitting insider [33]

Staff

Ethical Behavior and Issues
- IP Theft as a result of project attachment as if it belongs to them [2]
- IT Sabotage as a result of pressure or stress from management or colleagues [2, 3]
- Unwittingly leaking information or giving access and control to adversary over targeted assets [13]
- IT Fraud due to influence of competitors or other parties to achieve personal financial gain [2, 14]

Security Practice Negligence
- Operating upon DNS resolvers causing distributed denial of service (DDoS) attacks [15]
- Lack of attention for design inconsistencies between real and fake error messages [19, 23, 24]
- Failure to notice the absence of security indicators when they should be present [11, 26]
- Software updates are not applied to all devices, leaving gaps in the network's protection [17]

Work Pressure and Management
- Responding to phishing emails due to the presence of large work and email loads [11]
- The use of software without the review and approval of the organization (Shadow IT) [9, 18]
- Tendency to ignore the organization's warning notices against phishing attempts [23]

Security System Obstacles
- The company's security policies and procedures are considered incomplete or poorly defined [2]
- Employing standards around difficult inconvenient security systems processes [22]
- Lack of knowledge and use of padlock icon and HTTPS [26]

Situational Awareness and Training
- Lack of situational awareness of potential risks involved in clicking fake popups [26]
- Failure to recognize security measures installed in spoofed websites and web browsers [11, 26]
- Little training in visual deception that mimic legitimate text, images and windows [26]

Technology & Physical Events, Processes and Conditions

Software Exploits and Vulnerabilities
- Occurrence of buffer overflow corrupting or overwriting the valid data held in the system [19]
- Exploiting software vulnerabilities caused by software bugs and design flaws [19]
- Lack of continuous update to the system's current blacklist that is persistently out of date [31]
- Incorrect data validation leading to data corruption such as SQL injection [19]

Technical and Design Flaws
- The use of old wireless networks which rely on weak and less secure WEP encryption [14]
- Insider threat detection system classified normal activities as outliers [22]
- Designing computer-based algorithms focused on reliability without proper immunity to adversarial AI attacks [12]

Hardware Exploits and Vulnerabilities
- Adding a hardware trojan that might cause an error detection to accept inputs that should be rejected [17]
- Lack of security property library that can protect IP cores against hardware trojans [37]
- Exploiting weaknesses in the cryptographic system hardware such as power consumption [36]
- The use of untrusted hardware which in turn may contain harmful hardware-based Trojans (illegal clones) [19]

Operating Procedures and Conditions
- Lack of effective monitoring and tool to check for security standards compliance [29]
- Failure to prevent unauthorized devices or allowing its access up to 90 seconds [16, 17]
- Lack of mobile device management to promote user security awareness and poor safety hygiene [13]
- Implementing legacy systems or applications that are no longer supported by vendors and difficult to secure [16]

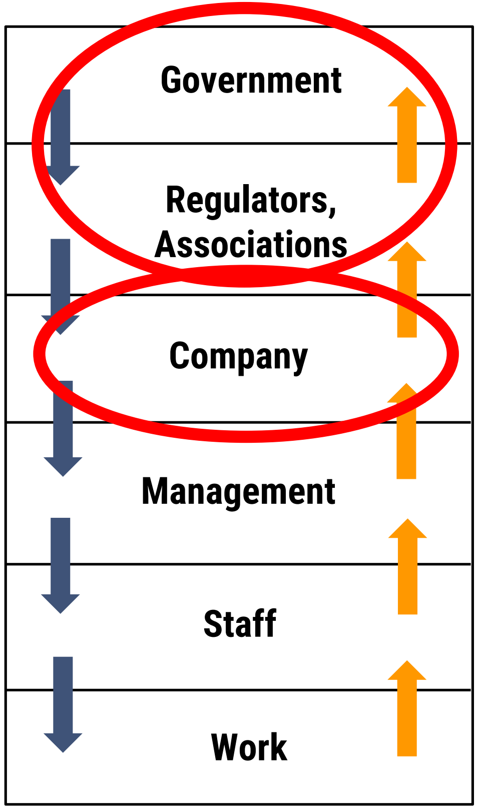
Outcome

Insider Threat Breach

ACCIMAP ANALYSIS

- Among internal-to-an-organization influencing factors, the company layer was found to be the root cause of questionable decisions made by management and personnel which contributed to insider threat.

- Among external-to-an-organization influencing factors, the layer of Government and Regulators was found to be crucial to security implementations in an organization since it mainly depends on the prosecution of laws, rules and regulations.



4

RECOMMENDATIONS

Promoting Security Culture

SECURITY CULTURE

ROLE OF ORGANIZATION

- The organization must allocate sufficient financial, technical and human resources to implement the assigned security responsibilities.

- The organizations must make arrangements for the regular review of their security practices and systems.

- The organization should coordinate with similar organizations to communicate security related information.

- A policy document is needed which states the commitment of the organization to security culture.

SECURITY CULTURE

ROLE OF MANAGEMENT

- Managers are responsible for initiating practices that comply with the organization’s security policies and objectives.
- Conduct self-assessments and arrange for independent audits of the management systems.
- Managers must ensure that training is conducted to develop skills and provide tools to promote and implement security culture.
- Managers need to encourage personnel to report any event that could affect the organization’s security culture.

5

CONCLUSION

Enhancing Proactive Capabilities

CONCLUSION

- The analysis of past insider threat incidents indicates that they were not caused by the "coincidence of independent failures and human errors", rather through the interactions of multiple involved contributing causes.

- There is a need to see and analyze the actions of workers or the errors that triggered an accident in a broader socio-technical context.

- The developed AcciMap provides a systemic view of accident causation that extends beyond the immediate causes. Rather it uncovers the aggregated factors throughout the system that promoted the conditions for the threat.

6

REFERENCES

REFERENCES

- Ponemon Institute. (2020). 2020 Cost of Insider Threats Global Report. Retrieved from: https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/proofpoint/ponemon-global-cost-of-insider-threats-2020-report.pdf (Accessed October 10, 2020).
- Branford, K., Hopkins, A., and Naikar, N. (2009). Guidelines for AcciMap analysis. In Learning from high reliability organisations. CCH Australia Ltd.
- Fischer, E. A. (December 12, 2014). Federal laws relating to cybersecurity: Overview of major issues, current laws, and proposed legislation. Congressional Research Service Report. Washington D.C, USA.
- The House Republican Cybersecurity Task Force. (October 05, 2011). Recommendations of the House Republican Cybersecurity Task Force. Retrieved from: https://www.gtscoalition.com/wp-content/uploads/2011/10/20111006-report.pdf (Accessed April 10, 2020).

REFERENCES

- Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., and Cowley, J. (May 2014). Analysis of unintentional insider threats deriving from social engineering exploits. In IEEE Security and Privacy Workshops: 236-250.
- Cappelli, D. M., Moore, A. P., and Trzeciak, R. F. (2012). The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley.
- Permanent Subcommittee on Investigations Staff Report (2019). Federal Cybersecurity: America’s Data at Risk. United States Senate. Committee on Homeland Security and Governmental Affairs.

California State University Northridge

SRA 2020 Risk Science for Sustainability

Thank You

Shorouk Bekir and Maryam Tabibzadeh

Contact info: shorouq.bekir.264@my.csun.edu

maryam.tabibzadeh@csun.edu