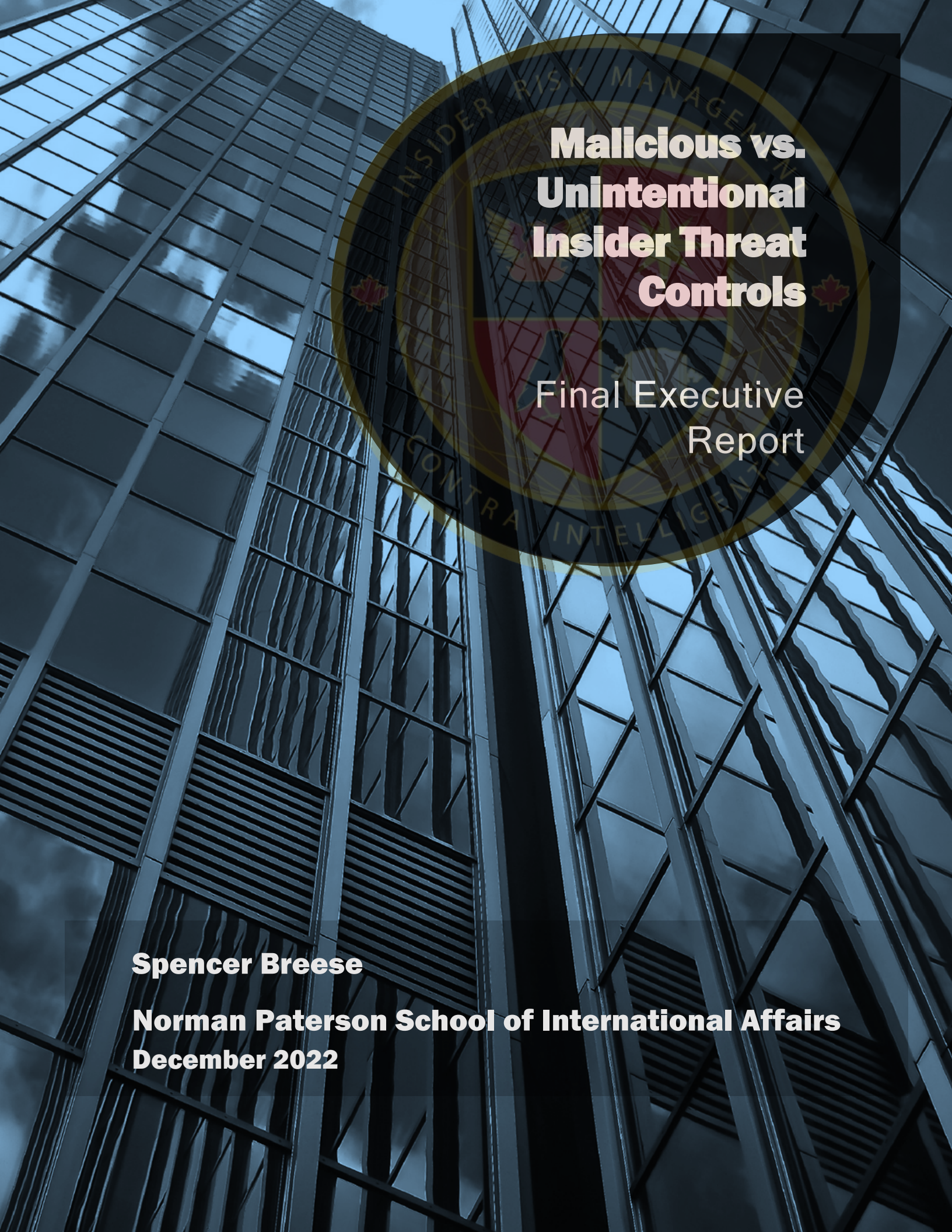

Malicious vs. Unintentional Insider Threat Controls

Final Executive Report

Spencer Breese

Norman Paterson School of International Affairs

December 2022

Executive
Summary

01 **Only two-third of respondents claimed that their organization had a clear definition of insider threats**

02 **Technical controls seem more targeted towards malicious threats, whereas organizational policies and programs on training and awareness were allocated towards unintentional threats**

03 **There were low levels of industry participation in this survey – information sharing across organizations and with academia should be further examined**

Background

Insider threats can be broadly separated into two categories: Unintentional, where the individual is unaware that they are committing an offense or opening up a system to malicious actors, and Malicious, where an individual intentionally commits an act against an organization with the intent of causing harm. Upon examination there is a clear gap between the occurrence of threat types and resource allocation towards various risk controls.

Research indicates that up to 87% of data breaches came from unintentional insider threats, rather than malicious actors. By comparison only a fraction of security resources are allocated towards reducing human error[1].

These trends have led us to hypothesize that organizations do not adequately differentiate their security controls between malicious and unintentional insider threats. A lack of differentiation means that risk controls are overly broad and do not appropriately address the differences between the two categories.

This study aims to broadly identify the differences between organizational approaches to insider threats, with a specific focus on assessing whether organizations effectively differentiate between malicious and unintentional insider threat types.

Research Questions

Do organizations effectively differentiate between risk controls required for malicious vs. unintentional insider threats? Does this create gaps within an organization's security strategy and lead to a false sense of resilience?

[1]As an example, in 2017, U.S. institutions allocated 0.62% of cybersecurity spending towards employee awareness training (Canham, Posey, & Bockelman, 2020).

Methodology

To investigate the differences in how organizations develop controls to prevent different forms of insider threats, a qualitative survey was sent out to industry professionals. The survey questions were based on present industry adopted standards relating to insider threat taxonomy, guidance and best practices utilized within organizations, security awareness training, and resource allocation invested towards different insider threat categories.

Results

The study suffered from a notable gap of low response rates (n<10). This suggests that there is additional work that must be done by Canadian academia and industry at large to normalize information sharing on the topic of insider threat to foster more applied research to enhance the resiliency of mitigation controls.

While the sample size in this study is not enough to draw significant conclusions, we were able to gain some insights of how organizations develop plans to prevent and mitigate insider threats. Key findings were:

- Organizations tend to obtain their definition of insider threat from a widely adopted professional standard, the most common being Carnegie Mellon. Sixty-six per cent of respondents said that their organization possessed a clear definition of insider threats.
- There is a clear differentiation between the allocation of technical controls and policies and programs meant to shape employees' behaviours within an organization's insider threat program. Technical controls seem to be more targeted towards preventing malicious threats (for example, network monitoring and SIEM use case development), whereas organizational policies and programs focused on training and awareness were allocated towards the reduction of unintentional threats (vs. guidance to employees on how to identify a potential malicious insider threat).
- Only one respondent indicated that the most significant insider threat identified by their organization would be categorized as unintentional.
- All respondents indicated that their organizations utilized methods such as gamification and workshops to provide "holistic" insider threat awareness training.

Conclusion and Next Steps

While a larger sample size is necessary to develop an understanding of organizational trends for insider threat controls, the results of the survey in this study could be used to influence the direction of future studies.

Areas of interest for future study direction include testing the effectiveness of technical controls vs. policy controls on different insider threat types (malicious vs. unintentional). Technical controls could be examined to see if they could be better attuned to prevent and mitigate unintentional insider threats, while policy and training and awareness programs could be examined to better address employee identification of malicious threats following organizational "trigger" events such as anticipated staff layoffs.

Industry-wide insider threat taxonomy could be compared. This could help determine if definitions provided by different academic and national government bodies are applied in a manner that allows different sectors of industry in Canada to operate more synergistically in their application of controls to mitigate the threat.

Finally, information sharing of insider risk mitigation best practices across organizations and with academic researchers should be further explored and discussed. This would help to better understand the low levels of participation as seen in this study. This would also assist organizations share their insights on successes and failures in trusted environments where the risk of compromised proprietary information is minimized.

Founded in 2022, the Canadian Insider Risk Management Centre of Excellence (C-InRM CoE) is an academic, private, and public partnership that generates academic research, provides training and apprentice opportunities, promotes knowledge sharing, and augments resources and capabilities in the professional market to mitigate insider threats to critical infrastructure.

The C-InRM CoE fosters an interdisciplinary approach to insider risk management towards the promotion of industry best practices and innovation within an evolving threat environment.

Funded by industry contributions and research grants, our products and services include research and analysis, facilitating workshops with subject matter experts, and generating lessons learned, built on a foundation of information sharing among a trusted community of security, intelligence, and defence professionals.