4/21/2021

Insider Risk for Canadian Financial Institutions

Ivan Barkar, Anthony Hope, Hayley Oyhenart, Darian Scherbluk

The Norman Paterson School of International Affairs

Introduction

Presentation Outline:

1. Methodologies
2. Literature Review
3. Analysis of Strategic Foresight Exercises
4. Examination of Industry Insights
5. Recommendations

Why should you be interested in insider risk?

Our Research Questions:

1. *What motivates insider risk events?*
2. *What are the components of a good insider risk program?*
3. *What gaps currently exist within the insider threat environment, and how do we address them?*
4. *What forward looking insider risk trends can we identify ?*

Methodology

Our Process...

- Literature Review
  - Built the baseline of understanding in the insider risk environment
  - Enabled contextualization of findings from the questionnaire, consultation, foresight exercises
  - Shaped our primary research design
- Questionnaire + Industry Consultations
  - Developed to understand participants' insights on the current and future landscape of insider risk and the efficacy of prevention/detection measures of insider risk
- Horizon Scan + Forecasting

Literature Review Findings

Academic Literature Recognizes...

- Behaviour/Social Human Factors (ex. Employee Satisfaction)
- Importance of Organizational/ Holistic Approaches (ex. Corporate Buy-In)
- Cyber and Technological Changes and Implications
- Legal Implications of all above elements in Preventing Insider Risk/Threats

Practitioner Literature Informs that...

- Insider risk is sector-agnostic + costly
- Can originate at every level
- Lacks forward looking perspective and does not account for future trends

Case Studies Discuss...

- Broad nature of insider risk/threats as well as cross-sectionality
- Work from home (WFH) implications

Horizon Scanning

Examining Forward Looking Approaches to Insider Risk

Scanning Results and Taxonomy

We collected **30 weak signals** that we used to inform broader trends and cross referenced them with our findings. This material informs the future landscape of insider risk **10-15 years from now.**

Examples of signals with extrapolation:

- Decentralized IDs through blockchain technology → Decreasing role of traditional networks/ endpoints?
- State hacktivism increases → Domestic govt. awareness/ corporate buy-in increases?

These signals essentially take the form of **three categories:**

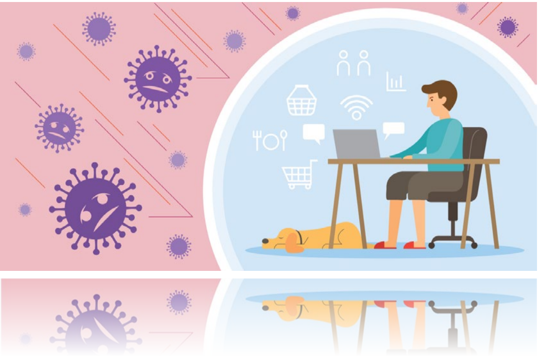
1. **Human Vulnerabilities/Changes**
2. **New Tech Risk/Threats**
3. **Political and Broader Global Change**

These categories are also found in the academic literature, suggesting future change along these traditional pathways is likely.

Insights Part I

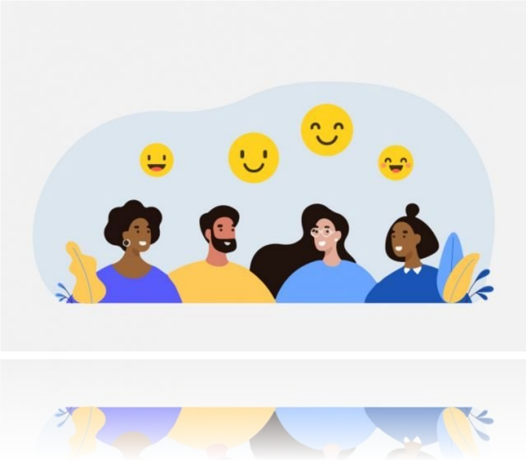
1. Work from home challenges

- Projected 8% increase in insider risk incidents as a result of work from home dynamics
- Elevated behavioural, technical, and organizational risks
- Work from home arrangements post-pandemic



2. Emphasis on personnel safety and satisfaction

- Employees with personal connection to the organization
- Balancing personnel focus with IT strategies



Insights Part II

3. Global and Political Attitudes on security are likely to play a key role on domestic insider threat landscape, corporate buy in and govt. initiative.

4. New technology will be implicated in **detecting and monitoring** employees to mitigate insider risk.

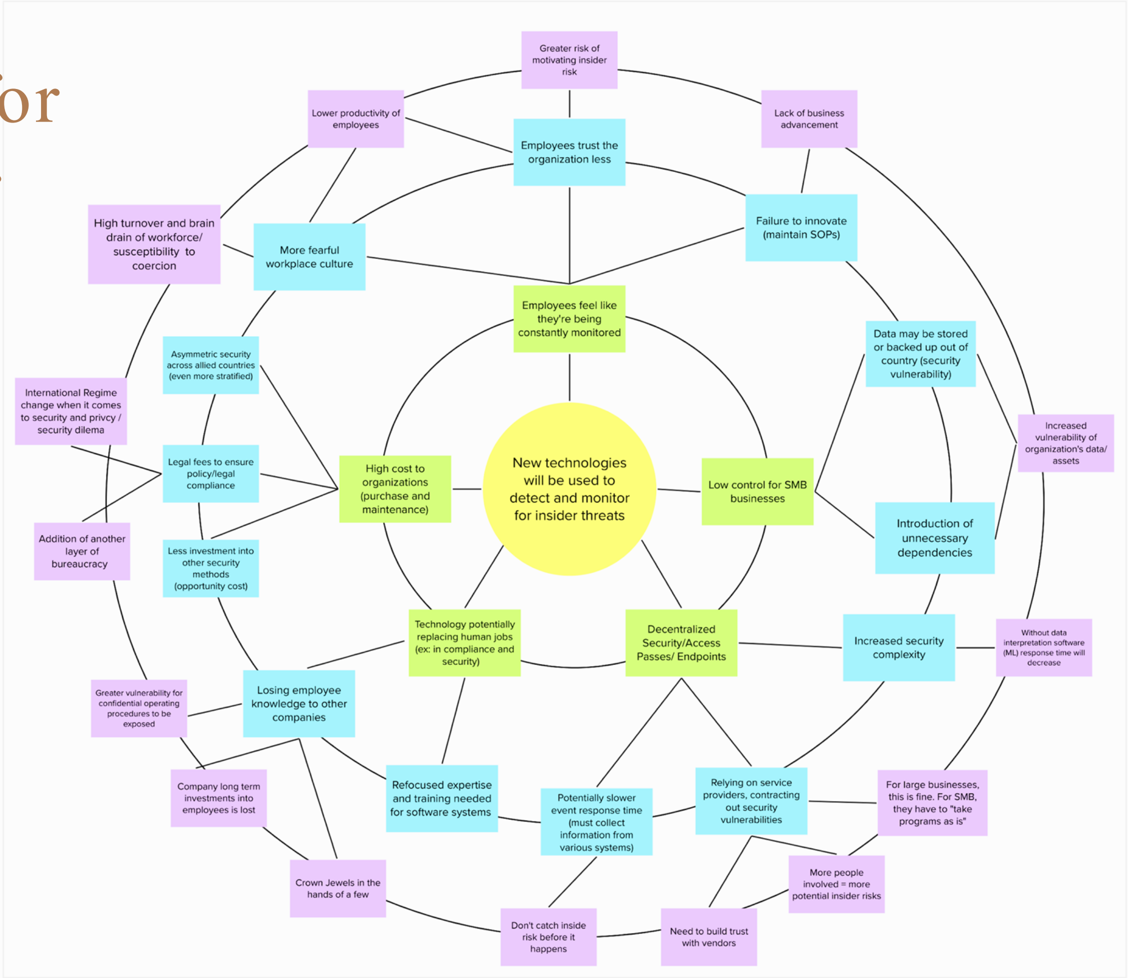
- **Ex. Blockchain/ New Decentralized Technology** will impact physical security considerations in insider risk

Forecasting Exercises

New technologies for the future of insider risk mitigation

- Impact on workplace culture
- Impact on innovation and advancement
- Reliance on managed service providers

- Main Takeaway: New technologies implicated in insider risk detection will affect workplace culture and the bottom line



New technologies will be used to detect and monitor for insider threats

Employees feel like they're being constantly monitored

High cost to organizations (purchase and maintenance)

Low control for SMB businesses

Technology potentially replacing human jobs (ex: in compliance and security)

Decentralized Security/Access Passes/ Endpoints

Greater risk of motivating insider risk

Lower productivity of employees

Employees trust the organization less

Lack of business advancement

Failure to innovate (maintain SOPs)

High turnover and brain drain of workforce/ susceptibility to coercion

More fearful workplace culture

Data may be stored or backed up out of country (security vulnerability)

Increased vulnerability of organization's data/ assets

Asymmetric security across allied countries (even more stratified)

International Regime change when it comes to security and privcy / security dilema

Legal fees to ensure policy/legal compliance

Introduction of unnecessary dependencies

Addition of another layer of bureaucracy

Less investment into other security methods (opportunity cost)

Increased security complexity

Without data interpretation software (ML) response time will decrease

Greater vulnerability for confidential operating procedures to be exposed

Losing employee knowledge to other companies

Refocused expertise and training needed for software systems

Potentially slower event response time (must collect information from various systems)

Relying on service providers, contracting out security vulnerabilities

For large businesses, this is fine. For SMB, they have to "take programs as is"

Company long term investments into employees is lost

Crown Jewels in the hands of a few

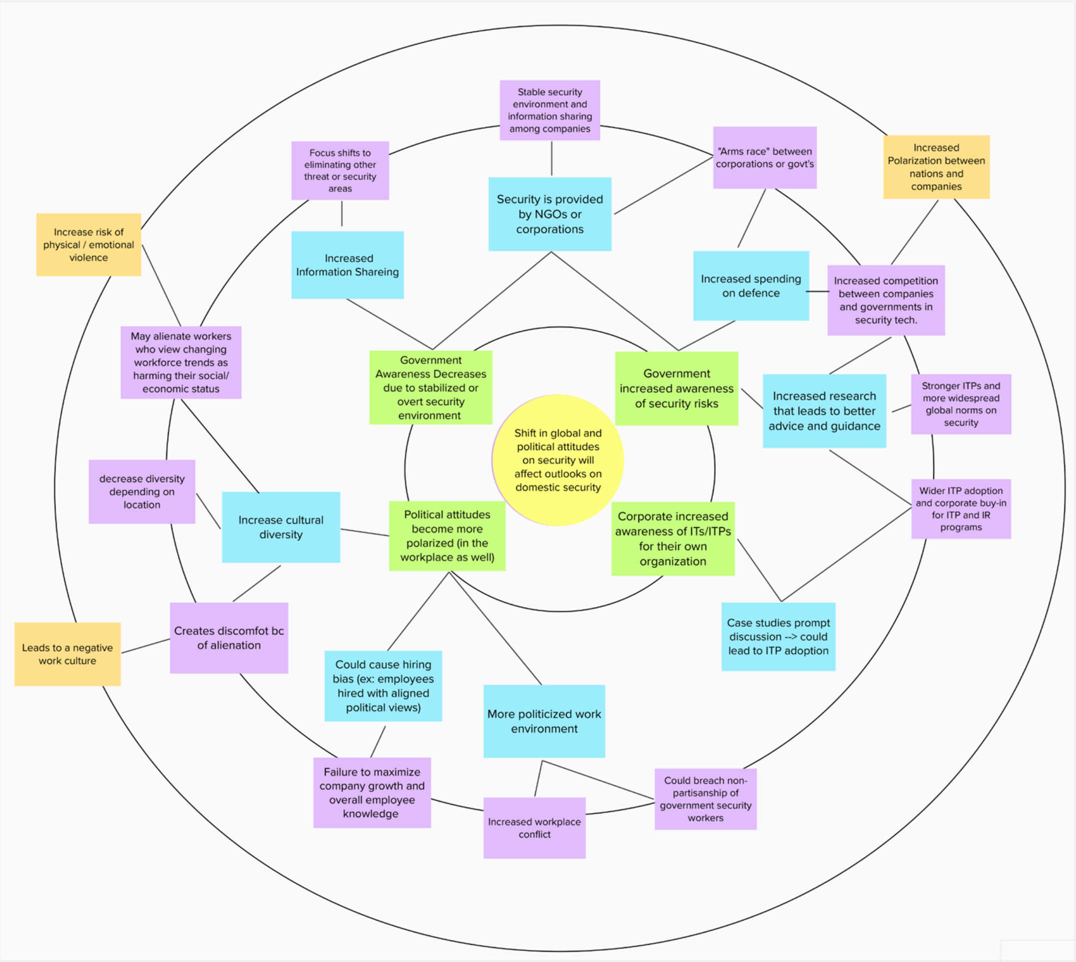
Don't catch inside risk before it happens

Need to build trust with vendors

More people involved = more potential insider risks

Shift in Global and Political Attitudes on Security

- Global attitudes will polarize security environment (one way or another)
- Securitization of insider risk
- Main Takeaway: Polarization of global political attitudes on security will negatively affect workplace culture and insider risk



Shift in global and political attitudes on security will affect outlooks on domestic security

Government Awareness Decreases due to stabilized or overt security environment

Government increased awareness of security risks

Political attitudes become more polarized (in the workplace as well)

Corporate increased awareness of ITs/ITPs for their own organization

Increased Information Shareing

Security is provided by NGOs or corporations

Increased spending on defence

Increased competition between companies and governments in security tech.

Increased research that leads to better advice and guidance

Case studies prompt discussion --> could lead to ITP adoption

More politicized work environment

Could cause hiring bias (ex: employees hired with aligned political views)

Increase cultural diversity

Creates discomfot bc of alienation

May alienate workers who view changing workforce trends as harming their social/ economic status

Stable security environment and information sharing among companies

Focus shifts to eliminating other threat or security areas

"Arms race" between corporations or govt's

Stronger ITPs and more widespread global norms on security

Wider ITP adoption and corporate buy-in for ITP and IR programs

Could breach non-partisanship of government security workers

Increased workplace conflict

Failure to maximize company growth and overall employee knowledge

decrease diversity depending on location

Increase risk of physical / emotional violence

Increased Polarization between nations and companies

Leads to a negative work culture

SUMMARY OF HORIZON SCAN

Similar trends uncovered in the literature, scanning, and our consultations

- Overlapping elements suggest that **change will be in established/known areas** such as IT/Human and potentially broader political spheres
- Insights **1&2 are overlapping with consults** and **3&4 are divergent with consults**

Future implications point to:

- **Importance of people and the social aspects** of both internal workplace culture as well as broader attitudes on security in society. This is supported by the case studies and consults, as well as the holistic nature of insider risks - effects are seen at every level and are derived from both individuals and political groups, or states
- **Awareness and education of new technology** is paramount because of the scale and pace of its evolution

This will be developed in further sections of research...

Expert Consults and Questionnaire

Practical Takeaways from Industry Stakeholders and Professionals

Data

- Questionnaire
  - Launched on LinkedIn in early March
  - Shared by industry professionals
  - 19 total responses; 14 valid; 5 excluded
- Consultations
  - Consulted 11 individuals
    - 5 government
    - 3 financial sector
    - 3 non-financial sector
  - 30 - 45 minute conversations
  - Guided questions mapped partially to questionnaire

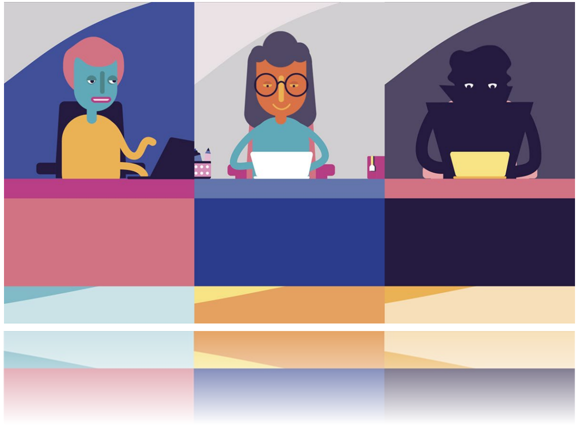
Considerations

- Time/budget constraints resulted in lower-than-predicted participation rates. Future research capstones and partnerships with Cdn. financial institutions could fix this issue.
- Questionnaire design assumed technology was a significant part of IRPs, did not ask about workplace culture
- Subject sensitivity meant consults had to exert caution to avoid divulging proprietary information

Who is an Insider Risk?

When it comes to motivations behind inside risk:

- Overwhelmingly, consult respondents identified **no** primary motivation (inside risk = mainly unintentional)
- For **malicious** inside risk, primary motivation is employee dissatisfaction with a negative work culture
  - Often coupled with secondary risk factors, such as financial gain
- Only two consults and six questionnaire respondents identified financial gain as **primary** motivator
- Any employee with access to proprietary information **can** be a liability



What makes a good Insider Risk Program (IRP)?

Findings from questionnaire/consults diverged

Questionnaire:

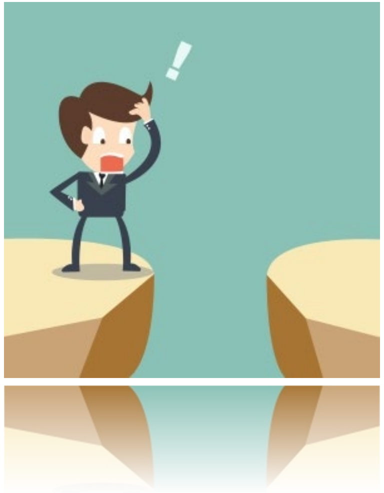
- Ability to protect client confidentiality and company data from insider attacks
- Ability to detect insider threat events and compromised assets
- Having a centralized insider risk framework
- Establishing an employee insider risk educational program
- Ensuring the physical safety of workplaces

Consults:

- First and foremost, IRPs need to be people-focused and empathy driven
  - Employee culture is critical, employees need to feel respected and have dignity in their work
- Good governance / executive buy-in (9.6/10 importance rating)
- Be adequately funded
- Regular security awareness training
- Technology as a supplemental yet necessary aspect to monitor for compliance

Current IRP Gaps

- Most individuals we spoke with **do not** have formal IRPs at their organization (¾ of survey respondents did)
    - Opt for a security operations centre (SOC) to monitor network and cyber security
- Many organizations focus on building a “security perimeter” - not inward focused
- Lack of executive buy-in a major concern
- Technology is prioritized over building a positive work culture
    - The “Big Brother” effect dampens employee satisfaction
- When technology is used, relevant data sources are not centralized
- Insider risk is becoming too broad



Emerging Risks

- COVID-19 pandemic introduced new security vulnerabilities, i.e. WFH posture (unanimous agreement)
    - Technology and data integrity preservation/protection
    - Employee satisfaction and work culture; mental health
    - Layoffs
- Band-aid fixes require permanent solutions
- Move to cloud concentrates data
- “Work from home is likely here to stay” - will need to incorporate into business continuity plans

Recommendations

Recommendations for Tackling Insider Risk

1) Build IRPs that are people-focused and that respect the dignity and privacy of all employees
2) Work towards a positive workplace culture that is empathetic, diverse and transparent
3) Use technology to supplement IRPs through monitoring and detection of anomalous behaviour based on preset baselines and in a transparent way, while also being conscious of Personal Information Protection and Electronic Documents Act (*PIPEDA*) constraints.
4) Increase training opportunities that encompass security and IT vulnerability awareness, workplace violence, and empathetic leadership

Thank you!

We can now take your questions.

CONTACT US:
Dr. Alex Wilner - AlexWilner@cunet.carleton.ca
Anthony Hope - anthonyhope3@cmail.carleton.ca
Ivan Barkar - ivanbarkar@cmail.carleton.ca
Darian Scherbluk - darianscherbluk@cmail.carleton.ca
Hayley Oyhenart - hayleyoyhenart@cmail.carleton.ca