EVERFOX

Insider Risk Challenge

Convincing Business Units to Act

by Dan Velez

The threats posed by a trusted insider can be catastrophic.

Goals & Strategy

1. Be the Insider Risk Thought Leader
2. Listen Carefully
3. Quantify the Risks of Insider Threats
4. Align with Business Goals and Demonstrate Return on Investment (ROI)
5. Explain the Types of Insider Threats and Offer Insider Risk Training
6. Highlight Regulatory Compliance & Alignment with the Organization's Cybersecurity Strategy
7. Present Mitigation Strategies
8. Highlight Technology Solutions
9. Focus on Strategic Champions
10. Emphasize Collaboration

Executive Summary

Recently, a colleague asked me,

> "I'm the new insider threat program manager. How do I convince the business units to act and help fund the insider risk management program?"

I thought the answer was obvious. Doesn't every business manager already know that the threats posed by a trusted insider can be catastrophic? Isn't there a front-page "another insider threat" article in the newspapers every few months? Everyone already cares or should care.

In pondering the question further, I considered that only some people eat and drink the insider risk nibbles feeding the subject matter experts. In a world where business unit directors are addressing project deadlines, acquisitions, cost cutting, and end-of-quarter profit forecasts, it's easy to see how they can overlook the invisible enemy within the business area. And suppose you're the newly anointed Insider Risk Program Manager. In that case, convincing business unit leadership to implement insider threat controls requires effective communication, clear presentation of risks, alignment with business goals, and showcasing the potential benefits. It's your job to make a compelling case for implementing insider threat controls within your organization and across lines of business.

Strategy

This paper suggests 10 best practices for the program leadership to engage and communicate the program goals, strategies, and benefits to the business unit and remind the program team to listen for and respond to common concerns and objections.

1. Be the Insider Risk Thought Leader.
You're in the role of Insider Risk Management Program Manager for a reason: you're the expert. Describe your experiences in insider risk management programs, your training, and the certifications you've earned. Highlight some of the lessons you've learned and the steps you took to address insider threats effectively.

Share some of your core beliefs that will guide your implementation, such as:

- "Our program will be supportive, not punitive."
- "It's a people program, not a cyber program."
- "Yes, we'll use technology, but we'll use it where it makes sense."

Keep it positive and focus on benefits

such as identifying and supporting employees who may be struggling with personal or financial problems that could make them vulnerable to exploitation by an attacker and supporting the culture of security within the organization, where employees are more likely to report suspicious activity.

You're selling yourself as soon as you walk through the door, and first impressions are essential. Be confident and prepared, using the rest of these tips as a guide, and remember to be approachable and open to adjustments and new ideas because your program must fit the company culture and each stakeholder group.

2. Listen Carefully
Before getting too far into your pitch, it's essential to understand the concerns and priorities of the business unit leadership. Ask the simple question, "What are your greatest concerns about implementing such a program?" and listen to the answer you receive.

Good listening skills can make you more persuasive:

- When you listen carefully to your stakeholder, you demonstrate that you value their thoughts and opinions, which is critical to your objective of making your stakeholder receptive to your message.
- When you better understand your stakeholder's perspective, you can tailor your message to their needs and concerns.
- Listening builds trust, and they are more likely to be persuaded by your arguments when they trust you.
- They have something important for you to learn about their corner of your organization. When you listen carefully, you are learning not only about their perspective but also how to get them to say "yes."

Be prepared for concerns of privacy and employee relations. Thoughtful and direct responses will demonstrate your deep understanding of the insider risk domain and will build confidence with your stakeholder. Finally, stress the supportive objectives of the program, not the punitive. No one wants the best thing about their company to be the insider "threat" program and the number of employees you hope to catch and dismiss.

3. Quantify the Risks of Insider Threats
Presenting relevant and concrete data from credible sources on insider threats' prevalence and potential impact is crucial to gaining buy-in from business unit leadership. Highlight real-world examples of organizations that have faced insider threats and the resulting financial, reputational, and operational consequences.

Examples:

- The 2023 Verizon Data Breach Investigations Report found that internal threat actors were involved in 19% of all data breaches. See page 13 for data that demonstrates that "internal" end-users show up twice as often as external State-sponsored attackers and page 46 for data showing that insiders are responsible for 99% of privilege misuse events, most often for financial gain (89%).
- The IBM Cost of a Data Breach Report 2023 asserts that the global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over three years.
- According to the Ponemon 2022 Cost of Insider Threats Global Report 2022, 67% of companies are experiencing between 21 and more than 40 incidents per year, representing an increase from 60 percent in 2020 and 53 percent in 2018. The problem is growing.

When speaking with leaders accustomed to making data-driven decisions, relevant and current data helps create a sense of urgency and demonstrates that credible and quantifiable concerns support your plans.

4. Align with Business Goals and Demonstrate Return on Investment (ROI)

Showcasing how implementing insider threat controls aligns with the business unit's goals and objectives is essential for gaining support. Emphasize how protecting sensitive data and preventing disruptions can lead to:

- Smoother operations. Insider risk management programs often identify procedural deficiencies or inefficiencies that drive employees to policy "gray zones" that increase the organization's risk while "trying to get the job done."
- Improved customer trust. By implementing a comprehensive insider risk management program, organizations demonstrate to their customers that they are committed to protecting their data and security. This commitment will increase customer confidence in the organization and its products and services.
- Stronger competitive advantage. A company with a robust insider threat program may attract and retain top talent, as employees are more likely to want to work for a company that is committed to protecting their data and security. Avoiding the costs associated with a data breach, such as lost revenue, regulatory fines, and damage to reputation, helps conserve limited resources that enable your organization to deliver competitive products and services.

A cost-benefit analysis outlining the potential return on investment (ROI) of implementing insider threat controls can be persuasive. Consider factors such as potential losses avoided, reduced incident response costs, enhanced brand reputation, and improved customer trust. Presenting a clear financial case for implementing controls can help business unit leadership understand the value proposition.

5. Explain the Types of Insider Threats and Offer Insider Risk Training

To help stakeholder leadership understand the scope of the problem, it's essential to explain the various forms of insider threats clearly. These can include unintentional mistakes, negligent behavior, and malicious actions. You can effectively convey the importance of implementing controls by providing examples and illustrating how each threat can impact the organization.

Explain that employee training and awareness programs help prevent insider threats and contribute to a culture of security and accountability. Provide examples of training modules or programs that the organization might implement to educate employees about the risks of insider threats and the importance of following security protocols. Emphasize the role of every employee in safeguarding the organization's assets.

6. Highlight Regulatory Compliance and Alignment with the Organization's Cybersecurity Strategy

If your industry is subject to regulations related to data protection and security, it's probably your most powerful twist of the arm, so highlight how insider threat controls can contribute to regulatory compliance:

- Explain the risks of non-compliance. Not complying with regulations can result in fines, penalties, and other sanctions. These can be costly and damaging to an organization's reputation.
- Show how investment can help to mitigate insider risks. By investing in the program, organizations can reduce the risk of intellectual property loss, data breaches, fraud, and other security incidents. This can help to protect the organization from financial losses, regulatory fines, and damage to reputation.
- Remind your stakeholder that compliance is the bare minimum. Regulations protect individuals and organizations from harm. However, they are often the bare minimum standard that organizations must meet. Forward-thinking organizations should not just comply with regulations but also strive to exceed them.

The following are regulatory compliance examples:

Financial Services

- Gramm-Leach-Bliley Act (GLBA): This U.S. law mandates that financial institutions must establish measures to protect the security and confidentiality of customer information, which includes guarding against insider threats.
- Sarbanes-Oxley Act (SOX): Although primarily focused on financial reporting and corporate governance, SOX indirectly encourages controls to prevent fraudulent activities by insiders through provisions that require accurate financial reporting.
- Federal Financial Institutions Examination Council (FFIEC) Guidelines: In the United States, the FFIEC issues guidelines and standards for financial institutions. The guidance includes recommendations for information security and insider threat mitigation.

- National Institute of Standards and Technology (NIST) Framework: NIST provides a framework for improving critical infrastructure cybersecurity, which includes addressing insider threats as part of a comprehensive risk management strategy.

- Payment Card Industry Data Security Standard (PCI DSS): While primarily focused on credit card data security, PCI DSS also has requirements that indirectly address insider threats, as controlling access to sensitive data is essential to compliance.

- Financial Industry Regulatory Authority (FINRA) Regulations: FINRA, in the U.S., provides regulations and guidance for broker-dealers and securities firms, including considerations for cybersecurity and insider threat controls.

- European Union's General Data Protection Regulation (GDPR): GDPR mandates organizations to protect personal data, which may include measures to prevent insider threats that could compromise data security.

Health Services

- Health Insurance Portability and Accountability Act (HIPAA): In the United States, HIPAA mandates the protection of patient health information (PHI) and electronic protected health information (ePHI). Healthcare organizations and their business associates must implement safeguards to prevent unauthorized access, including from insiders.

- Health Information Technology for Economic and Clinical Health (HITECH) Act: HITECH extends HIPAA's privacy and security provisions, requiring covered entities and business associates to implement measures to secure electronic health information and report data breaches.

- General Data Protection Regulation (GDPR): In the European Union, GDPR mandates the protection of personal data, including health data. Healthcare organizations must implement appropriate security measures, including insider threat controls.

- Health Canada Regulations: In Canada, Health Canada provides regulations and guidelines for protecting health information, including measures to address insider threats and safeguard patient privacy.

- International Organization for Standardization (ISO) Standards: ISO 27799 and other relevant ISO standards offer guidance on information security management in healthcare organizations, including considerations for insider threat mitigation.

Cybersecurity Frameworks

Common cybersecurity frameworks include requirements or recommendations to implement insider threat controls as part of a comprehensive cybersecurity strategy. Insider threats are recognized as a significant risk to organizations, and addressing these threats is a crucial aspect of protecting sensitive data, systems, and operations. While the specific wording and emphasis on insider threat controls may vary between frameworks, general principles such as least privilege, secure configurations, and auditing and monitoring remain consistent.

Here are some well-known cybersecurity frameworks that typically include considerations for insider threat controls:

- NIST Cybersecurity Framework: The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a flexible framework to manage and reduce cybersecurity risk. It includes the "detect," which identifies unauthorized internal activities. Insider threat controls are implicit within the broader threat detection and monitoring context.

- ISO 27001 and ISO 27002: The ISO 27001 standard focuses on information security management systems, while ISO 27002 provides guidelines for implementing specific controls. These frameworks emphasize the need for access controls, user awareness and training, incident response plans, and monitoring user activities to detect unauthorized or malicious actions.

- CIS Critical Security Controls (CIS Controls): These controls provide prioritized actions designed to improve an organization's cybersecurity posture. Several of the controls are relevant to insider threat mitigation, including control 12 (Boundary Defense), control 16 (Account Monitoring and Control), and control 17 (Data Protection).

- NIST Special Publication 800-53: This publication provides a catalog of security and privacy controls for federal information systems and organizations. It includes controls related to insider threat detection, access controls, auditing and accountability, and security training and awareness.

- FAIR (Factor Analysis of Information Risk): While FAIR is more focused on risk analysis and assessment, it can be integrated with other frameworks to evaluate insider threats' potential impact and likelihood. It helps organizations make informed decisions about resource allocation for insider threat controls.

- MITRE ATT&CK: You may find it important to frame your insider risk management plans using the MITRE ATT&CK framework. The Insider Threat Research & Solutions team[1] at MITRE isn't a fan of this approach and is developing a new framework. Still, you will find some guidance at MITRE Engenuity [2]website that will enable you to adjust the description of your plans using the ATT&CK lexicon of TTPs and the accompanying detection and mitigation strategies.

Lastly, your company may have certain contractual obligations to formalize insider risk management programs as is required for work with the U.S. Department of Defense or other components of the government.

While insider threats may not always be explicitly called out in every regulation or framework, the underlying principles of access control, user monitoring, employee training, incident response planning, and awareness are essential components of managing insider threats effectively.

7. Present Mitigation Strategies

Lay out specific insider threat controls and strategies to implement within the organization. These could include access controls, user monitoring, employee training, incident response plans, and security awareness programs.

Explain the benefits and effectiveness of each strategy and how they contribute to mitigating insider threats. Be sure to highlight the need to align and adjust technical and organizational controls to create a holistic approach to managing human risk by:

- Using the latest security technologies.

- Conducting regular security assessments.

- Training employees on security best practices.

- Creating a culture of security within the organization.

8. Highlight Technology Solutions

Your stakeholder may need to be made aware of the insider risk management technology landscape or may be concerned about the costs or burdens that come with them. If your immediate program plans call for introducing technologies:

- Describe how you have arrived or will arrive at their requirements and features .

- Describe how you are going to measure and manage their impact on the program, organization, and users.

- Be sure their capabilities are not overstated; underpromise and plan to over-deliver.

- Explain how these solutions complement existing controls and enhance the organization's overall security posture.

Here are examples of technology that can support insider risk management:

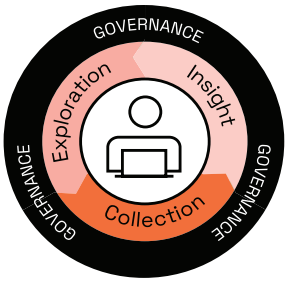
- Data loss prevention (DLP): DLP solutions can monitor for and prevent accidental or ambivalent removal of sensitive data.

- User and entity behavior analytics (UBA) solutions: UEBA can monitor employee behavior for suspicious activity, such as excessive access to sensitive data, abuse of system privileges, or threats of harm.

- Identity and access management (IAM) tools: IAM tools can manage employee access to data and systems to prevent unauthorized access and to help provide non-repudiation.

- Encryption: Encryption can protect sensitive data from unauthorized access.

- User activity monitoring (UAM) capabilities: UAM can feed UEBA solutions, detect specific behaviors of concern, and support investigations of anomalous user behavior. IAM supports attribution to users and non-repudiation.



1 https://insiderthreat.mitre.org/
2 https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/insider-threat-ttp-knowledge-base/

9. Focus on Strategic Champions

Moving about the organization to build consensus, you may run into components with members who are hard to persuade or resistant to change. To overcome this challenge, identify the stakeholders among them who are most likely to be supportive of your ideas. Build relationships with these stakeholders and get to know them and their concerns. Be willing to listen to their feedback and be open to their ideas and suggestions. These are your strategic champions.

Strategic champions will then help you build momentum, overcome resistance to change, and communicate your message effectively and in a way that resonates with the other stakeholders. Strategic champions can help you to get things done.

By focusing on strategic champions, the insider risk program manager can increase their chances of success in convincing stakeholders to act.

10. Emphasize Collaboration

Insider risk management is a team sport, so invite the business unit to the next Insider Risk Management Steering Group meeting. Bring in IT security experts, legal advisors, compliance officers, and other relevant stakeholders to lend their expertise and answer any technical or regulatory questions business unit leadership might have. Collaborating with these experts helps build credibility for the proposed insider threat controls and ensures alignment with industry best practices and legal requirements.

Describe how effective insider threat controls require collaboration across departments, creating an opportunity to strengthen teamwork and communication within the organization:

- Executive leadership: Executive leadership must set the tone for insider risk management by communicating the importance of the program and providing the necessary resources.
- Human resources: Human resources must develop and implement policies and procedures to operationalize critical organizational controls such as background checks, onboarding, and employee termination activities.
- Legal and Privacy: Your program must achieve an equitable balance between organizational interests and employee privacy and liberties.
- IT security: IT security must implement technical controls, such as data loss prevention and user behavior analytics, to prevent and detect insider threats.
- Business units: Business units must identify and mitigate insider risks specific to their operations. For example, a business unit handling sensitive customer data must implement different controls than a business unit developing sensitive technology.

These cross-functional stakeholders can create a comprehensive insider risk management program that protects the organization from harm. Still, the business unit must be involved to ensure the security of sensitive information systems and protect the whole organization.

Summary

Remember that effective communication from a confident program leader is key to convincing your business units to act:

- Be clear and concise: Your business case should be easy to understand and take little time to describe.
- Use data and evidence to support your claims: The business case should be based on data and evidence, not just assumptions.
- Tailor the business case to your audience: The business case should address the specific needs and interests of your audience.
- Get feedback on the business case from other stakeholders before you finalize it.

By following these tips, you increase the chances of convincing your stakeholders to act, which will help you to secure funding, generate buy-in, and implement an effective insider risk management program.

Effective Communication with Stakeholders is Key

Learn more @ Everfox.com »