Gartner Research

Strategies for Midsize Enterprises to Mitigate Insider Risk

Paul Furtado

19 April 2023

Gartner

Strategies for Midsize Enterprises to Mitigate Insider Risk

Published 19 April 2023 - ID G00788550 - 7 min read

By Analyst(s): Paul Furtado

Initiatives: Midsize Enterprise Technology Leadership

> One of the biggest threats to any business is the one that walks through the front door every day. Midsize enterprise (MSE) CIOs must prioritize the security risk represented by employees, contractors and integrated third-party partners as part of a comprehensive security program.

Overview

Key Findings

- End users in MSEs often demonstrate poor judgment specific to cybersecurity.
- MSEs often lack the capability to effectively monitor the risks associated with employees, contractors or third-party partners.
- Limitations in security capabilities and resources make incidents attributed to insider activity difficult to predict, identify and contain.
- Data breaches caused by abuse of access often take months or years to detect data breaches caused by abuse of access.

Recommendations

To combat the insider risk, the MSE CIOs must:

- Implement the “rule of three” to mitigate risk while effectively using limited security resources.
- Establish an enterprisewide culture of security by developing an insider threat security team composed of personnel from key areas of the organization.
- Mitigate the insider risk by implementing behavioral technology and sound governance practices.

- Make insider risk mitigation manageable by focusing on and monitoring high-risk assets and accounts.

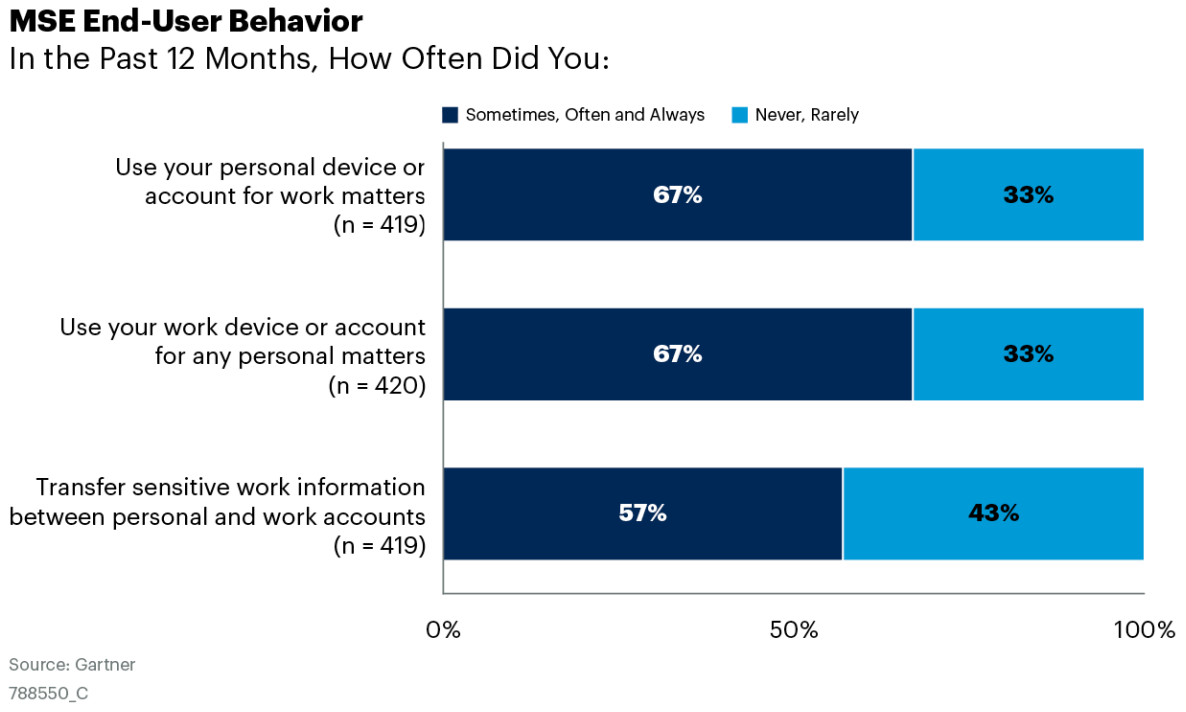
Strategic Planning Assumption

By 2025, insider risk will cause 50% of organizations to adopt formal programs to manage it, up from 10% today.

Introduction

Whether through error, negligence or malice, employees, contractors and integrated third-party partners represent risk that must be addressed. The problem lies in the fact that insiders have an advantage over an external attacker — they know where the data exists and where to get it. Insider behavior (see Figure 1) coupled with lax governance puts midsize enterprises at a greater risk. In this instance, size and scale can work to the advantage of MSE technology leaders. For example, a typical MSE supports 900 employees, and as a result IT teams tend to have more intimate knowledge of the insider behavior and patterns. For the purpose of this research, an insider is classified as any employee, contractor or integrated third-party partner with access to internal systems.

Figure 1: MSE End-User Behavior



When MSE technology leaders think of threats to their business, more often than not they consider them to be malicious in nature. This thinking can often be misleading as insiders are 2.5 times more likely to make an error or have a lapse in judgment than to maliciously misuse their access, [1] and when security incidents occur as a result, they take an average of 85 days to contain. [2]

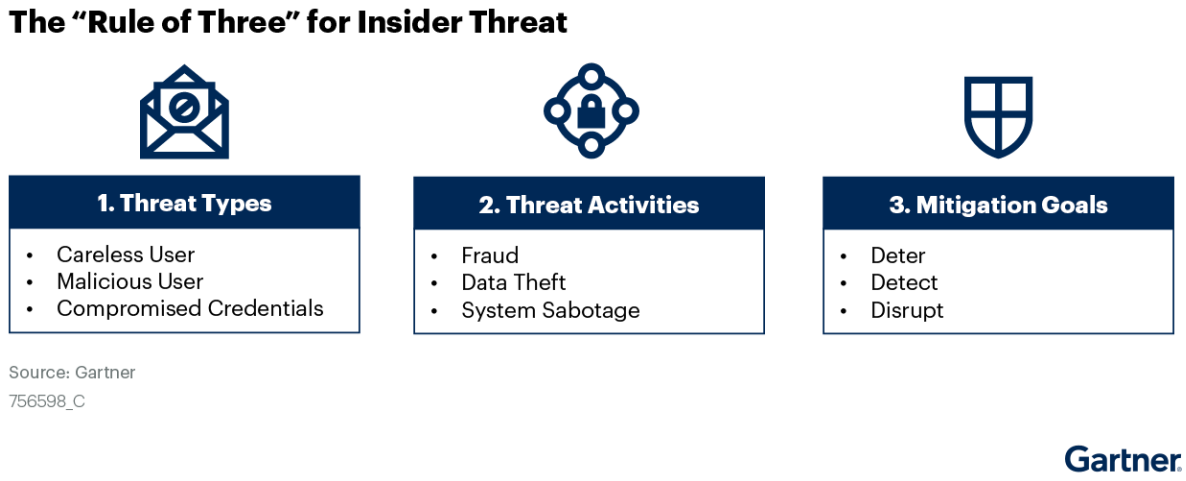
> **"Not every insider risk becomes an insider threat; but every insider threat started as an insider risk."**

Analysis

Implement the Rule of Three for Insider Risk

To effectively mitigate insider risks, MSE technology leaders must think, act and behave pragmatically. A simple, yet practical way to look at an insider risk program is using The Rule of 3 for Proactive Insider Risk Management (see Figure 2).

Figure 2: The "Rule of Three" for Insider Threat



Insider threats can then be classified as one of the following three types of threat actors:

- **Careless user** — Accidentally exposes sensitive and/or proprietary data (including errors and improper configurations)
- **Malicious insider** — Intentional sabotage or data theft for either personal reasons or financial gain

- **Compromised credentials** — Credentials exploited by someone inside or outside the organization for the purpose of data theft and/or sabotage

Insider threat activities are typically categorized into one of these three activities deemed to be a policy violation or illegal by law:

- **Fraud** — Such as phishing or financial theft
- **Intellectual property theft** — Such as customer lists or confidential data
- **System sabotage** — Such as malware, ransomware, account lockouts or data deletion

Lastly, on a macro level, the rule of three for insider threats focuses on three core mitigation goals intended to:

- Deter the individuals from wanting to do it in the first place
- Detect the activity
- Disrupt the effort

To use the guidance of the rule of three effectively, MSE technology leaders need an insider threat mitigation program that is composed of people, processes and technology. All three elements are required to be successful.

Establish a Culture of Security by Developing an Insider Threat Security Team

Insider threats cannot be stopped by the IT group alone. They require the support and input from the executive team, legal department and HR. Enterprise support is important, because the MSE technology leaders will be dependent on other business groups and leaders to provide governance enforcement in addition to information on staff transition/turnover, contractor engagements and vendor access requirements.

Having the support of the executive team and a cross-functional security team will help with early identification of high-risk users. Implement a confidential, formal notification process that managers, business leaders and HR can use to notify IT security about upcoming disciplinary actions or terminations with employees and/or contractors. Use the same process for notifications when an employee/contractor voluntarily submits their resignation. Any of these scenarios could be a catalyst for the employee, contractor or vendor to exfiltrate sensitive materials from the organization or sabotage enterprise systems.

Mitigate Insider Risk With Technology and Sound Governance Practices

When entering into agreements with trusted business partners, all contracts should include requirements for insider threat protection that meet the standards or regulatory requirements for your organization. There must be a mechanism for denying access to users whose behavior may negatively impact your business without requiring termination of the contract (at your discretion).

Include insider threats as part of your end-user awareness training. Encourage employee participation in notifying IT security about suspicious behaviors and provide confidential mechanisms for them to do so. Be transparent in terms of informing the user base that activities are monitored.

Implementing automated tools and technology with embedded behavioral technology will simplify administration and management.

MSE technology leaders who currently do not have a mature insider threat management program will need to invest in tools and technology. Some tools that help automate the detection and mitigate the risk of insider threats are:

- Data loss prevention
- Endpoint protection platform
- Identity access management
- Mobile device management
- Multifactor authentication
- Privileged access management

- User and entity behavior analytics

These tools will help identify potential risks. However, a human element is still required to act on alerts in a timely fashion and within the agreed-on governance processes.

Not all indicators of insider threats are technology-based. Physical activities could indicate potential prohibited activities. Have some folks changed their routines and started coming in early or leaving after hours when no one else is around? Have they accessed other parts of the facility where they typically don't go? Have they been seen printing large amounts of material? Do they seem to have suddenly become affluent? Each of these, in combination with other factors, could raise suspicion and be used to consider the individual a high-risk insider threat. Leverage existing technologies (such as video cameras and card readers) to help spot these anomalous behaviors.

Most insider threats can be mitigated by doing the small things right. Focus on some low-cost and no-cost options to help thwart insider threats:

- Awareness training
- Bring-your-own-device policies
- Identify erratic behavior
- Log monitoring
- Vendor management
- Wi-Fi security

Make Insider Threat Mitigation Manageable by Focusing on and Monitoring High-Risk Assets and Accounts

Ideally, MSE technology leaders would measure activities of all accounts against known baselines. This can be costly and time-consuming to do in-house as it is not best practice for MSEs to build out dedicated security groups. Partnering with a managed security service provider (MSSP) is the recommended method for MSE to overcome these resource obstacles.

Where there is no budget for an MSSP service or resources to monitor all accounts, you can still implement monitoring for high-risk accounts. You must define what constitutes a high risk for the business. Create a list of high-risk targets and activities to monitor. In some cases, a user/account may be considered high risk due to a change to their normal behavior patterns or employment status. Once they are no longer deemed to be a threat, remove them from the monitoring platform.

Examples of high-risk accounts:

- Administrative accounts
- Contractors
- Employees changing departments
- Employees connecting after hours
- Employees who have received disciplinary or performance improvement notices
- Employees who have submitted resignations
- Third-party partners
- Service accounts

When it comes to activities, you need to spend some time upfront to create baselines so you have something to measure against. Significant changes to any of the following metrics could be potential indicators of problematic behaviors:

- Average data egress to device (local hard-disk drive, external storage, etc.)
- Average access requests blocked per account
- Average web traffic by account
- Average number of email attachments
- Average email attachment size
- Average data sent to third-party storage (Box, Dropbox, Microsoft OneDrive or Google Drive)

The MSE technology leaders can implement an insider risk mitigation program without putting excessive burden on limited resources by limiting the monitoring of activities to known high-risk accounts.

Evidence

2022 Gartner Drivers of Secure Behavior Survey: This survey was conducted via an online platform from May through June 2022 among 1,310 employees across functions, levels, industries and geographies. The survey examined the extent to which employees behave securely in their day-to-day work, root causes of insecure behavior, and the types of support and training that they received from their organizations to drive desirable secure behaviors. We used descriptive statistics and regression analysis to determine the key factors that drive or impede employees' secure behaviors and develop cyber judgment.

[1] 2022 Data Breach Investigations Report, Verizon.

[2] 2022 Ponemon Costof Insider Threats Global Report, Proofpoint.

Document Revision History

Strategies for Midsize Enterprises to Mitigate Insider Risk - 29 October 2021

Strategies for Midsize Enterprises to Mitigate the Insider Threat - 17 January 2020

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

The Rule of 3 for Proactive Insider Risk Management

Market Guide for Insider Risk Management Solutions

Security Staffing Options for Midsize Enterprises

Quick Answer: How Can Midsize Enterprises Benefit From Security Vendor Consolidation?

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for midsize enterprise leaders:

Roadmap

2024 Technology Adoption Roadmap for Midsize Enterprises

Benchmark your technology adoption plans against your midsize enterprise peers.

Download Now

Infographic

2024 CIO Agenda: A Midsize Enterprise Perspective

Learn top priorities, technology and challenges for midsize enterprises in 2024 to deliver on digital initiatives.

Download Now

eBook

3 Must-Haves in Your Midsize Enterprise Cybersecurity Incident Response Plan

Improve your organization's ability to be prepared for a cybersecurity incident.

Download Now

Tool

IT Score for Midsize Enterprise CIOs

Measure the effectiveness of your IT operating model and highest-priority activities.

Download Now

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights

Attend a Gartner conference
View Conference

Gartner®