Strategies for Midsize Enterprises to Mitigate the Insider Threat

Published 17 January 2020 - ID G00451251 - 7 min read

By Analysts Paul Furtado

Initiatives:Midsize Enterprise IT Leadership

The biggest threat to any business is the one that walks through the front door every day. Midsize enterprise CIOs must prioritize the security threat employees, contractors and integrated third-party partners represent as part of a comprehensive security program.

Overview

Key Challenges

- Cybersecurity within midsize enterprises (MSEs) is perceived as solely an IT responsibility.
- MSEs often lack the ability to effectively monitor risks associated with employees, contractors or third-party partners.
- Security incidents attributed to insider activity are difficult to predict, identify and contain.
- Data breaches caused by abuse of access typically take months or years to be detected.

Recommendations

To combat the insider threat, the midsize CIO 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 threat risk by implementing behavioral technology and sound governance practices.
- Make insider threat mitigation manageable by focusing on and monitoring “high-risk” assets and accounts.

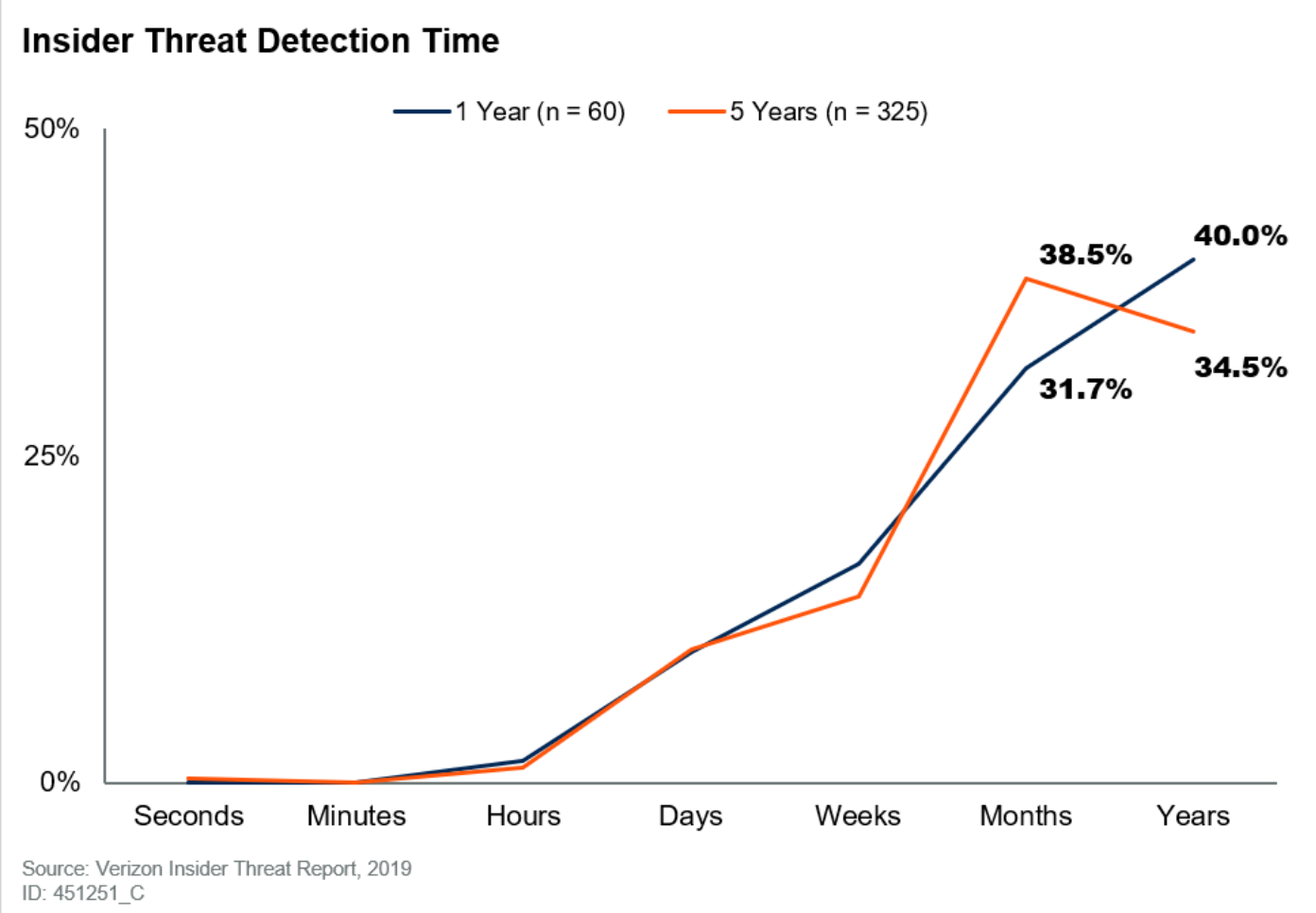
Introduction

Whether through malice, negligence or error, the security threats posed by employees, contractors and integrated third-party partners 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.

For the purpose of this research, an insider is classified as any employee, contractor or integrated third-party partner with access to internal systems.

Insider threats put the midsize organization at a greater risk due to the time span in which they typically go undetected. Over 70% of breaches that begin with an abuse of access are only found months or years later (see Figure 1).

Figure 1. Insider Threat Detection Time

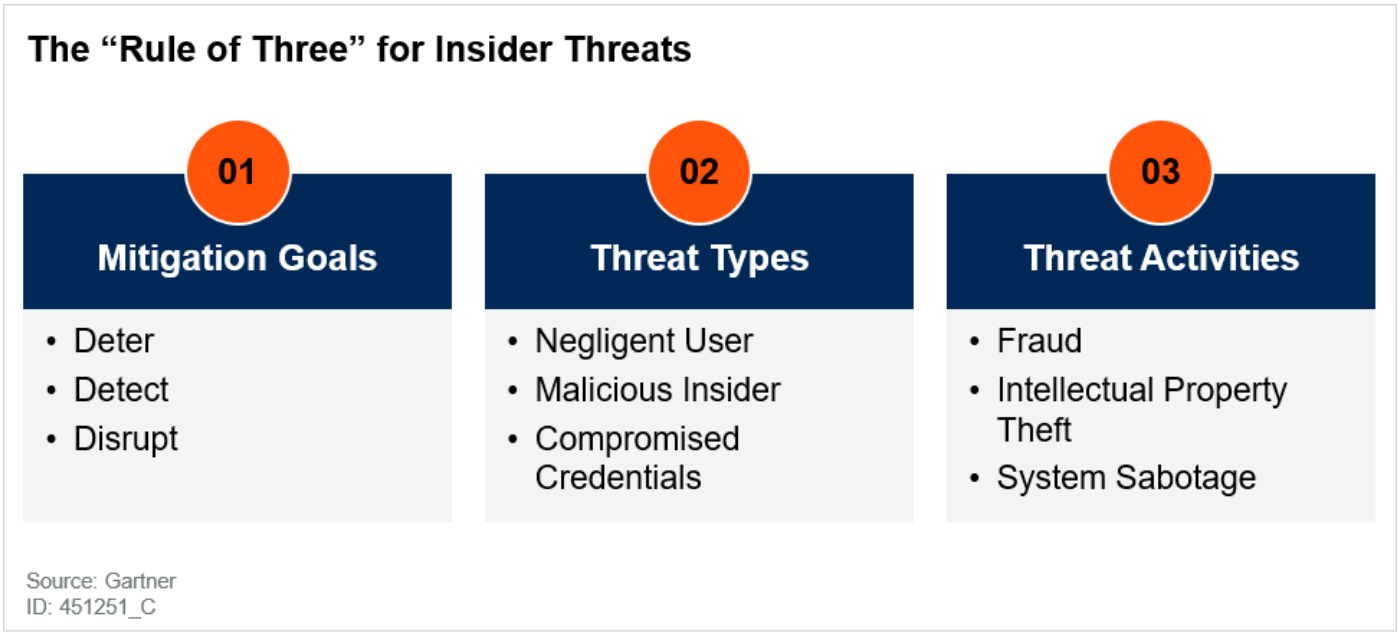


Analysis

Implement the Rule of Three for Insider Threats

To effectively mitigate insider threats, MSE CIOs must think, act and behave pragmatically. A simple yet practical mitigation program focusing on the three core mitigation goals is an effective means to that end. The "rule of three" will enable MSE CIOs to mitigate a significant amount of risk while making the most effective use of a limited pool of security resources (see Figure 2).

Figure 2. The "Rule of Three" for Insider Threats



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

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

- **Negligent user** — accidentally exposes sensitive and/or proprietary data (including errors and improper configurations)
- **Malicious insider** — intentional sabotage, data theft for either personal reasons or financial gain
- **Compromised credentials** — credentials exploited by someone outside the organization for the purpose of data theft and/or sabotage

Lastly, 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

To implement the rule of three effectively, MSE CIOs need an insider threat mitigation program that is composed of people, processes and technology. All three are required in order to be successful.

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

Fifty-seven percent of MSEs do not have a chief information security officer or dedicated IT security leader; [1] therefore, insider threats cannot be stopped by the IT group alone. It requires the support and input from the executive team, legal department and HR. Enterprise support is important because the MSE CIO 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 and a cross-functional security team will help with early identification of high-risk users. Implement a confidential 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 Threat Risk by Implementing Behavioral 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 telling the user base activities are monitored.

> **Implementing automated tools and technology will simplify administration and management.**

Midmarket CIOs 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 (DLP)
- Endpoint protection platform (EPP)
- Identity access management (IAM)
- Mobile device management (MDM)
- Multifactor authentication (MFA)
- Privileged access management (PAM)
- User and entity behavior analytics (UEBA)

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-upon 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 (video cameras, card readers, etc.) 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 (BYOD) 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 CIOs would measure activities of all accounts against known baselines. This can be costly and time-consuming to do in-house for CIOs without dedicated cybersecurity resources.

Partnering with a managed security service provider (MSSP) would be the recommended method to overcome these 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 high-risk activities to monitor. In some cases, a user/account may be considered high risk as a result of a change to their normal behavior patterns or employment status. Once they are deemed to no longer 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 metrics below could be a potential indicators of problematic behaviors:

- Average data egress to device (USB, local hard-disk drive, 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, Google Drive, etc.)

Limiting monitoring of activities to known high-risk accounts allows the MSE CIO to implement an insider threat mitigation program without putting excessive burden on limited resources.

Evidence

[1] 2017 Midsize End-User Baseline survey:

Gartner conducted this research from April through June 2017 in order to examine what midsize enterprises are doing differently to succeed with fewer resources when it comes to investing and deploying technology. In total, 607 CIOs or most senior IT leaders in a midsize organization were qualified and surveyed. Of the completed interviews, 53% were achieved online (322 surveys) and an additional 47% (285 surveys) were achieved via telephone interviews.

Recommended by the Author

How to Build Incident Response Scenarios for Insider Threats

How to Respond to the 2019 Threat Landscape

Insider Threat Detection: Specialized User Behavioral Monitoring

Recommended For You

It's Time to Give into Shadow IT

SLA Builder

Midsize Enterprises Should Embrace MDR Providers

Four Experiments Midsize Enterprises Should Run in 2019

Midsize Enterprises Must Prioritize to Achieve Effective Vulnerability Management