Bottomline™

Inside Insider Threats

3 CHALLENGES AND 3 APPROACHES TO ADDRESSING THE DANGER WITHIN

The numbers are anything but reassuring. Insider threat incidents are on the rise. Corporate email is being used to steal sensitive data. Credential theft is skyrocketing. It is taking longer to contain threat events, which means the cost to organizations is going up.

Businesses are at the center of a perfect storm. Greater problems than ever before from insider threats demand a greater response in order to detect and contain them – ideally, before damage is done. The good news is that next-generation solutions exist and can provide this desperately-needed protection.

3 Challenges that Contribute to Insider Threats

When surveying the rise of insider threats, it is appropriate to ask "Why now?" Why are insider threats on the rise? Why are malicious insiders achieving their aims so frequently? Why have institutions struggled to keep up? Three challenges contribute to where we are today.

50%

insider threat incident increase over two years*

1. Work Looks Different Now

The first challenge that fuels the problem is that we are working differently today. Chiefly, remote, hybrid, and work-from-home (WFH) business models were launched into overdrive courtesy of the global pandemic. This makes it difficult for organizations to monitor and control how employees handle sensitive data. It is easier for employees to create opportunities to compromise data when they are working without direct supervision.

Hand-in-hand with new employee work models, there has been a proliferation of personal devices under Bring Your Own Device (BYOD) policies. Employees who use their own devices can readily access sensitive data for malicious purposes if those devices are not properly secured.

65%

increase in cost to organizations due to credential theft*

The risk of insider threats is also increased by outsourcing globally, working extensively with service providers, and bringing in outside contractors. While such third parties are not employees of an organization, they are effectively insiders since they have access to company systems, applications, and data.

As a general rule, fraud always flows to a place that is less protected. The increase in new business models, BYOD devices, and third-party involvement has opened up vulnerabilities that bad actors have been swift to take advantage of.

As a general rule, fraud always flows to a place that is less protected

2. Technology Looks Different Now

The rapid – almost fantastical – rate of change in technology comprises the second challenge for businesses when it comes to insider threats. Businesses are contending with disruption caused by:

- **Complex Environments:** Organizations have increasingly complex IT environments with numerous applications and data repositories spread across on-premise deployments and both private and public clouds. Managing and securing these environments is a formidable task; any gaps in protection allow insiders to exploit vulnerabilities or access sensitive information.
- **Data Proliferation:** Organizations collect and store massive amounts of information, making it difficult to keep track of who has access to what. This data proliferation not only is exploited by bad actors, but can increase the potential for unintentional data leakage as employees may not fully understand the sensitivity of all the data they handle.

* Ponemon Institute, 2022 Cost of Insider Threats

Businesses are experiencing regulatory pressure on two fronts

- **Data Exfiltration:** Malicious insiders leverage advanced tools and techniques to exfiltrate data. This includes using encryption, anonymization, and obfuscation methods to hide their activities. These tools are readily available on the dark web and make data theft hard to detect.
- **IoT Devices:** The proliferation of Internet of Things (IoT) devices in both homes and workplaces has introduced new potential attack vectors. Insiders may exploit IoT vulnerabilities to gain access to networks and data.
- **Big Data:** Organizations use big data and analytics to process and analyze vast amounts of information. While this can help detect insider threats, it also means that malicious insiders may blend in with the background noise, making it harder to identify their activities.
- **Alert Overload:** As insider threat management solutions strive to keep up, they often generate a huge volume of alerts, a significant percentage of which are false positives. This overload causes alert fatigue and can distract investigators from serious crimes.

It is a truism with new technologies that, along with the benefits they provide, they often have darker sides that create or exacerbate risk.

3. Regulations Looks Different Now

A third challenge in responding to insider threats is that businesses are experiencing regulatory pressure on two fronts.

On the one hand, various countries and regions have enacted cybersecurity laws that mandate the implementation of robust security measures. These laws often require organizations to protect against insider threats by putting in place access controls, encryption, monitoring, and reporting mechanisms. There are also industry-specific regulations that require compliance, including HIPAA in healthcare, GLBA in financial services, and NERC CIP in energy. Additionally, regulatory pressure is extending to organizations' responsibilities for third-party vendors and suppliers: companies are expected to ensure that their partners have adequate insider threat prevention measures in place. Failure to comply with applicable regulations can leave doors open for malicious insiders.

Simultaneously, however, businesses are facing the need to obey increasingly strict data privacy regulations. Of particular note, the General Data Protection Regulation (GDPR) in the European Union imposes strict requirements on organizations to ensure that insider threat monitoring complies with data privacy. For example, employers must be transparent with employees about the monitoring activities. This includes informing employees about the types of data being collected, the purposes of monitoring, and the methods used. Additionally, the principle of data minimization requires that organizations only collect and process the minimum amount of data necessary for the intended purpose. Insider threat management tools must therefore be carefully configured to collect and analyze only relevant data. Compliance with these regulations can potentially inhibit an organization from capturing data that could detect insider threats.

$17.19 Million

average organizational cost for incidents that took over 90 days to contain*

* Ponemon Institute, 2022
Cost of Insider Threats

3 Approaches that Counter Insider Threats

Overcoming these challenges and countering insider threats requires that businesses employ robust approaches to investigation, data, and analytics that incorporate next-generation technology solutions.

1. Prioritize The Resources For Investigation

The first challenge that fuels the problem is that we are working differently Many organizations have strong teams, processes, and technologies in place to deal with various types of external fraud, such as account fraud, payment fraud, identity theft, and wire fraud. Insider threat management capabilities, however, can lag behind. It is not uncommon for an external threat team to be given the task to handle insider threats as well, under the assumption that "a threat is a threat." Processes may not exist for critical aspects of detection and containment, such as how to appropriately confront an employee about suspicious behavior. Worst of all, organizations often lack insider-threat- specific technology. To counter insider threats, businesses need to recognize the distinct nature of these threats as compared to external dangers.

COMPLEXITY AND DETECTION CHALLENGES

External threat solutions typically focus on identifying known attack patterns and vulnerabilities, which can be straightforward to detect and mitigate.	Insider threats often involve trusted individuals within an organization who may have legitimate access to sensitive data and systems. Distinguishing between normal behavior and suspicious activities can therefore be very difficult.

DATA ACCESS AND MONITORING

External threat solutions often concentrate on monitoring network traffic, system logs, and known malware signatures.	Insider threat management requires monitoring and analyzing user behavior, which can be resource-intensive and may require more advanced solutions like User and Entity Behavior Analytics (UEBA).

DATA ACCESS AND MONITORING

External threat solutions mainly focus on identifying and blocking malicious activities from external actors.	Insider threats typically involve individuals with varying motives, ranging from unintentional mistakes to malicious actions. Detecting malicious intent can be challenging and may involve looking at a broader context of user behavior.

INTEGRATION AND COLLABORATION

External threat solutions do not require extensive collaboration from internal departments and can be more isolated in their operation.	Effective insider threat management often requires close collaboration between IT, security, human resources, and other departments. This coordination c an be complex to establish.

With these distinguishing characteristics in mind, organizations can take best practices from external threat detection and adapt them for insider threat management. This includes making it a priority to:

- **Establish a dedicated insider threat management team** with employees who have the necessary expertise to navigate the balance between security and privacy, analyze complex behavioral data, and conduct investigations with discretion.
- **Define processes for insider threat detection and containment** to clearly outline matters such as the collection and documentation of evidence, what internal departments need to be involved when confronting an employee, and how to mitigate intentional and unintentional threat situations.
- **Leverage leading-edge technology** that centralizes management dashboards, tools, and capabilities to capture data, analyze information, and support investigations into insider threats. Solutions should be able to address threats to data, applications, and systems residing on the mainframe, web, and SaaS.

By addressing insider threats with the same rigor and resources applied to external threats, businesses can better safeguard their data, their customers, and their reputations.

Capture more data & Transform unstructured data into structured data

2. Expand The Scope Of Data

the scope of data coverage, both by collecting more data and by creating structured data from unstructured data.

There are three primary ways to collect data. First, there is log-based data capture. Log files record basic user actions such as login and logout times, access to files and directories, changes to files and data, and system commands executed. They also capture a wide range of system and network events, such as firewall activities, network connections, system configurations, and software installations. However, because they are event-focused, log files do not record non-event employee activities such as making inquiries or browsing customer information.

They also do not provide significant context around log entries.

Agent-based data capture relies on agents or software components installed on individual endpoints, servers, or devices to monitor and capture data related to user activities, system configurations, network traffic, and other relevant events. Agents bring data capture down to individual user actions including keystrokes, mouse movements, application usage, and file access. They also can provide a fair amount of context around user activities to help investigators assess risk and intent. That being said, agents cannot obtain the actual field values that appear on the screens an employee looked at or interacted with. These values therefore cannot be incorporated into analysis.

85 days

mean containment time for an insider incident*

* Ponemon Institute, 2022 Cost of Insider Threats

Finally, there is next-generation **network-based data capture**. In this non-invasive approach, user activity on business-critical systems and applications is captured for analysis directly from the corporate network, regardless of application type or whether data resides on premise or in the cloud.

Network-based data capture both expands the scope of the data collected and creates structured data from unstructured data. Its capabilities include:

- **Capturing every user action** within a monitored business system or application, including activities such as searches, queries, and browsing.
- **Creating a visual screen-by-screen record** of user activity that can be "replayed" like a movie, giving investigators vastly expanded context for assessing employee behavior.
- **Extracting field values from the screens an employee accessed** to create structured data that can be fed into the analytical engine.

3. Deepen The Insights From Analytics

When more data is collected overall and unstructured data is transformed into structured data, the third approach to insider threats becomes possible: deepening the insights gained from analytics.

Network-based data capture both expands the scope of the data collected and creates structured data from unstructured data.

Log-based and agent-based analytics provide rich insights for investigators, including behavioral profiling of users and endpoints to learn what constitutes normal behavior and flag deviations, file integrity monitoring to track changes to files and directories at a granular level, and network traffic analysis to provide insights into communication patterns and potential security risks.

Network-based analytics can do all of this plus deliver entirely new categories of insights by employing capabilities such as:

- **Field data analysis** that extracts the values of the fields on the screens an employee accesses to create a highly-detailed profile of user behavior. This enables investigators to pinpoint where users are viewing or interacting with business/ customer data in potentially inappropriate ways.
- **Auto-mapping of screens** to identify important fields on a given screen and prioritize alerts for any anomalous activity that involves those fields. This helps investigators allocate their time for maximum effectiveness.
- **Link analysis** that draws upon field values and cross-segment network data to visualize user behavior. This allows investigators to make connections between diverse activities such as an employee making a query, updating account information, and initiating a payment.

The augmented data capture and analytical capabilities of network-based insider threat management also support investigators by providing increased documentary evidence with which to make a case against an employee or initiate legal action.

Succeeding in a Complex Digital Landscape

The decision to move relationships or add services must be executed swiftly and efficiently in The escalating risk posed by insider threats is a pressing concern for businesses today as organizations grapple with the challenges of an evolving work environment, rapid technological advancements, and stringent regulatory requirements.

However, by prioritizing the allocation of resources for insider threat investigation, expanding the scope of data capture, and deepening insights with advanced analytics, businesses can effectively detect and contain incidents. Next-generation technologies such as network-based insider threat management will play a key role in these approaches, empowering businesses to protect their data, their customers, and their reputations in an increasingly complex digital landscape.

To learn more, contact Bottomline today

Contact Us

Bottomline

REV US013024LM

Corporate Headquarters
100 International Drive, Suite 200
Portsmouth, NH 03801
United States of America

Phone: +1 603-436-0700
Toll-free: +1 800-243-2528
info@bottomline.com