Insider Threats:

The Danger Within

Research Brief

IBM

govloop

Introduction

Most federal employees think their agencies are safe from insider threats – but they're wrong. A 2017 Meritalk survey found that 42 percent of federal cybersecurity professionals said that their agencies were the target of cyber incidents perpetrated by insiders.

The U.S. Computer Emergency Readiness Team (US-CERT) defines insider threats as any "current or former employee, contractor, or other business partner who has or had access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity or availability of the organization's information or information systems."

This range makes predicting insider threats hard and stopping them harder. Insider threats commit fraud, computer infrastructure sabotage and the theft of confidential or commercially viable information from organizations. They can lurk undetected within an agency indefinitely, and even well-meaning individuals can accidentally become one in certain circumstances.

To better understand the current climate, GovLoop partnered with IBM, a leader in mitigating and protecting against insider threats, for this research brief. In the following pages, we analyze a survey of 170 federal employees about their views on insider threats and share solutions to better protect against them. We also spoke with IBM experts, including Ian Doyle, Business Unit Executive, Cybersecurity Strategic Growth Initiatives; John McLaughlin, Executive Security Architect; and Tim McMillan, Executive Security Strategist.

1 Name for Many Problems

"Insider threat" is an ambiguous phrase, as it denotes any individual with access to an organization's insider information. Insiders can intentionally harm their agencies, or they may do so unknowingly. The term also fits outside parties like business associates and contractors. People who feel safe from insider threats are often confused about what the term means, leaving them unaware they're in danger.

"The biggest misconception is that insider threats are not a problem," Doyle said of federal agencies. The truth is they should be an agency's top priority.

The most notorious insider threats deliberately damage their agencies by attempting or committing actions like espionage, sabotage and terrorism. They may also willfully disclose classified or sensitive information.

"They're trying to be malicious," Doyle said. "They're trying to take your most sensitive data and expose it."

Other insider threats lack bad intentions. Many instead disclose classified, controlled, proprietary or sensitive information without permission.

"Insider threats always exist," Doyle said. "Any person within an organization could introduce an insider threat problem by carelessly clicking on something."

Insider threats are insidious, as some remain undetected for weeks, months or years. This invisibility leaves many government employees believing their agencies are safer than they are.

"It can be hard to distinguish insider threat behavior from normal behavior," McLaughlin said. "It's easy to cover up."

McLaughlin added that potential insider threats include general users, privileged users who can change their security policy, third parties with or without the same security maturity as both and even frustrated workers.

> *"Any person within an organization could introduce an insider threat problem by carelessly clicking on something."*
>
> — Ian Doyle, Business Unit Executive, Cybersecurity Strategic Growth Initiatives

Understanding the Landscape

GovLoop surveyed 170 federal employees about the perceptions of insider threats and how their agencies are protecting against them. The results reveal a federal workforce that could improve its understanding of the challenge.

Seventy percent said that their agency had never experienced an attack or breach related to an insider threat, while 30 percent said that their organization had suffered one (See Figure 1). This result surprised Doyle, who suggested respondents are unaware of the frequent danger facing them or don't fully know what encompasses an insider threat.

"An insider threat is something that hurts the organization," he said. "It's not something that you want making the front page of the news. If something is found, it's taken care of quickly, discretely and with as minimal impact as possible."

Thirty-seven percent of those who had experienced an insider threat ranked a malicious outsider or contractor as their agency's biggest challenge. Thirty-five percent chose unintentional employee actions, and 28 percent said a malicious employee (See Figure 2).

Despite these statistics, 54 percent said insider threats are not a rising challenge at their organization, while 46 percent said they are (See Figure 3).

Sixty-one percent said that dealing with insider threats is a priority at their agency, while 39 percent said that it's not (See Figure 4).

"What that's really telling us is that 39 percent are operating below the bar on insider threats," Doyle said. "You should always strive for 100 percent."

Figure 1

Has your agency ever experienced an attack or breach related to an insider threat?

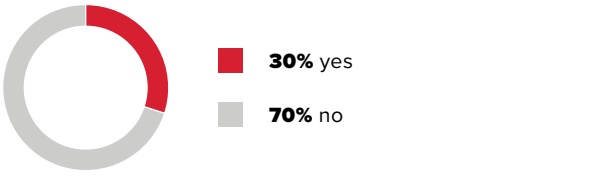


Figure 2

If yes, which type of insider threats have been the biggest challenge for your agency?

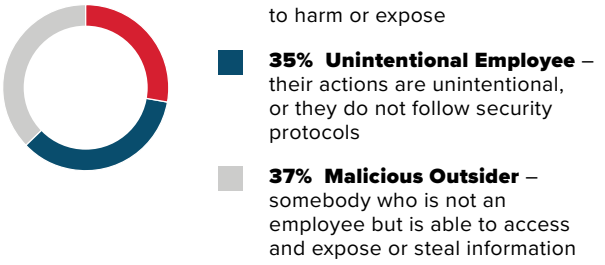


Figure 3

Are insider threats a rising challenge at your agency?

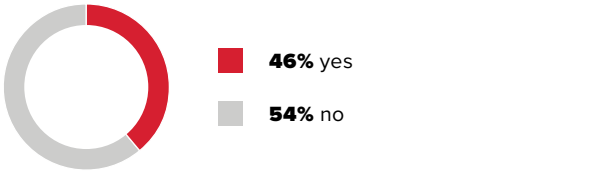
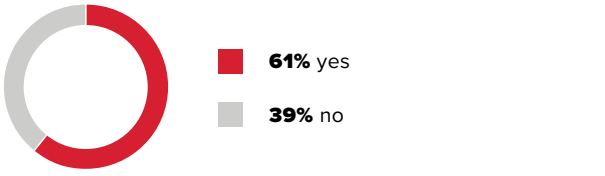


Figure 4

Is dealing with insider threats a priority at your agency?



Respondents listed budget, lack of leadership buy-in, lack of skills, competing with other priorities, higher-ranking cybersecurity issues and other problems as reasons their agency was not prioritizing insider threats. Of these, 47 percent cited more important cybersecurity worries as the main challenge (See Figure 5).

Most participants considered their agency's insider threat prevention and detection methods to be average or better. Seventy-nine percent ranked their agency a three or higher on a five-point scale (five being very effective). This means 21 percent said it was not effective (See Figure 6).

While the results are positive, McMillan said that unfortunately, many organizations don't realize their insider threat strategy is lacking until their defenses fail.

"In every breach, exfiltration or data corruption, we look back forensically and investigate the incident to discover that the indicators were already there," he said. "They actually resided within our network for an extended period."

Insider threats should always be a top cybersecurity priority for agencies due to the potential damage they cause.

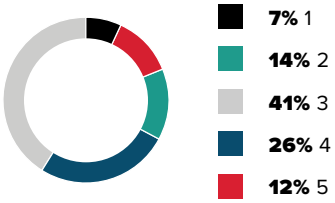
It's not just about monitoring network traffic anymore, or end points," McMillan said. "It's anything and everything that could become a hot spot for how an adversary will gain access to an organization's information.

Figure 5

If insider threat is not a priority, why?

Figure 6

How effective do you consider your agency's insider threat prevention and detection methods to be? (1 is not effective at all, 5 is very effective)



Preparing for the Worst

Recognizing the danger of insider threats, former President Barack Obama issued E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," in 2011. It tasked the heads of all federal agencies accessing or operating classified computer networks with implementing an insider threat detection and prevention program. The order also established the federal Insider Threat Task Force for fighting the problem governmentwide.

Although federal agencies are required to have insider threat programs, defending against them is more than a compliance exercise. There are several questions agency leaders should be asking:

- **Is critical data completely monitored and locked up with limited access?**
- **Are you monitoring the behavior analytics of all your employees, including federated employees, contract workforce etc.?**
- **Do you have a formal incident response plan in place?**

The survey found that 61 percent said their agency has a formal incident response plan with insider threat provisions, while 11 percent are developing one. With that said, 27 percent are still lacking one and don't have a plan to develop one (See Figure 7).

Fifty-nine percent have a department or team for monitoring and/or responding to insider threats, while 41 percent do not (See Figure 8).

Forty-six percent rated their agency's insider threat program as adequate but needing work, while 27 percent ranked it as immature and 27 percent called it advanced (See Figure 9).

Figure 7

Does your agency have a formal incident response plan with provisions for insider threat attacks?

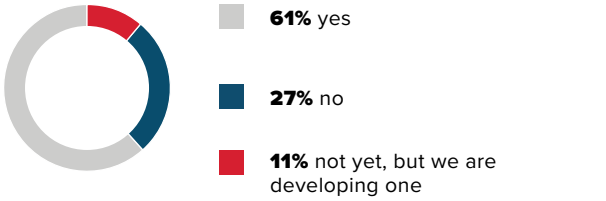


Figure 8

Does your organization have a dedicated team or department responsible for monitoring and/or responding to insider threats?

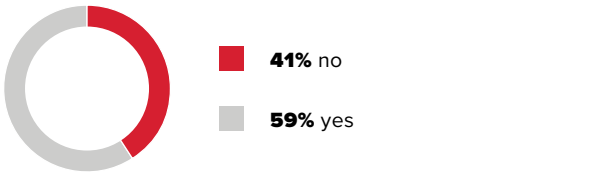
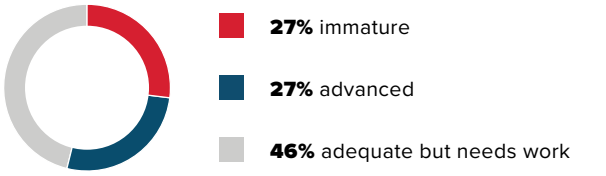


Figure 9

How would you rate the state of maturity of your insider threat program?



Insider threats will never stop presenting agencies with cybersecurity challenges because the threat continues to evolve. But there are solutions agencies can use to help.

The survey asked about new tactics being used in the federal government to minimize insider threats. The survey found that behavior analytics is the most common new tactic agencies are using, with 50 percent utilizing it, followed by super user monitoring (39 percent) and enterprise intelligence analysis (38 percent). Other tactics the survey asked about include machine learning (30 percent), predictive analytics (26 percent) and crown jewel monitoring (12 percent) (See Figure 10).

Behavior analytics offer agencies another arrow in their quivers by establishing and scrutinizing users' activity patterns. Robust behavior analytics is a powerful defense against insider threats, as it can discern the intent behind actions.

Super user monitoring is the surveillance of users with privileged access to valuable assets beyond a regular user's.

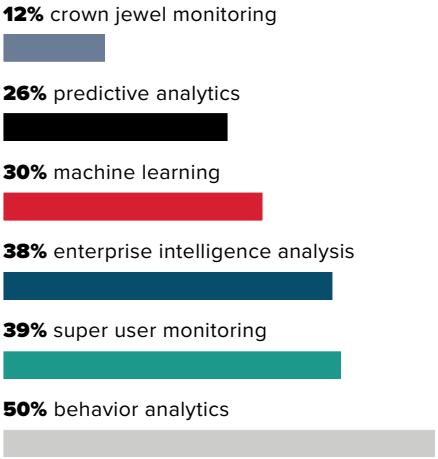
Crown jewel monitoring is vigilance over an organization's most prized resources. Enterprise intelligence analysis detects and understands actionable patterns within an entire agency's information.

More specifically, **analytics** can be applied to discovering and interpreting meaningful behavior in an organization's workforce. Predictive analytics makes forecasts about future events using data patterns. Machine learning uses statistics so that computers are trained to comprehend data without requiring explicit human intervention.

Even with these new tactics, Doyle said that an agency's response to insider threats should be a collaborative process, as it requires an enterprise effort best-suited for its mission requirements.

Figure 10

What new tactics are your agency trying to minimize insider threat? (select all that apply)



Data Security and Identity Management

Battling insider threats begins with continuously examining an agency's network and fully understanding the data stored on it.

"It's controlling, monitoring and encrypting the data itself," Doyle said. "It's a data security strategy that protects all of the databases across the enterprise. But protecting critical data is just one facet of a larger insider threat program."

Agencies can also encrypt their data and determine which users access it. Multiple controls exist for handling daily security operations, including encrypting, monitoring and securing data.

Appointing asset privileges to specific users and then monitoring their activities versus those of normal users is another valuable tactic.

Beating Insider Threats with Behavior Analytics

"Behavior analytics is something that is going to be deployed more readily across government agencies," McMillan said. "User analytics, those applications and tools, will give them a broader and better picture of insider threats."

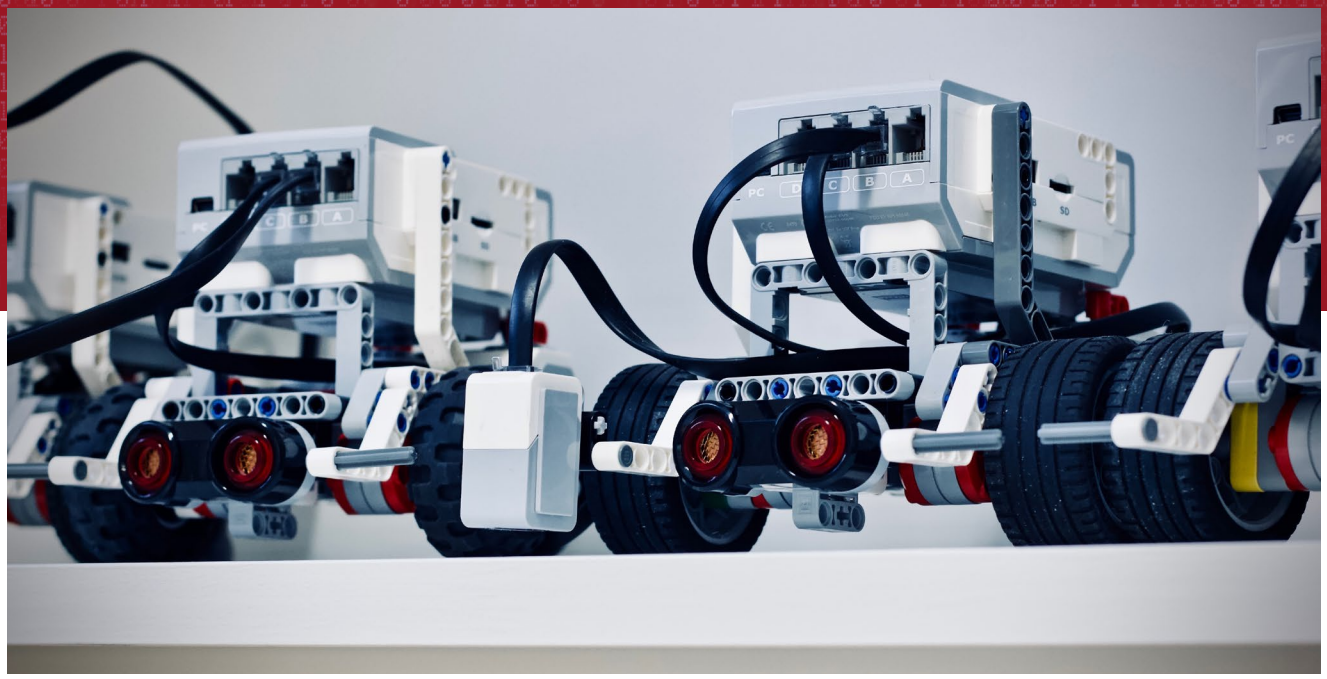
McMillan noted that many organizations contend with unconnected applications and lack the ability to comprehend the entirety of their users' actions.

"If the money I'm spending on security applications and tools is for these disparate, stovepipe parts that don't talk to each other, then I don't have the ability or authority to analyze the true operations of my enterprise," he said of agencies.

Behavior analytics thwarts insider threats by analyzing the integration between human resources, travel and security control data. A person booked for air travel elsewhere, for example, would not use their credentials to enter a building in a different location. This scenario could indicate unauthorized behavior and a potential insider threat.

Another example involves examining a user's credentials and logs to determine whether they are using the proper device. An unauthorized log-in may be an insider threat.

"Humans follow strict patterns of behavior," Doyle said. "You're looking for abnormal behavior. It's that first alert that it's something to look at before it potentially becomes an issue. Behavior analytics is critical in the scheme of insider threats."



The AI Revolution and Insider Threats

The rise of big data increases the danger that insider threats present agencies. More data means more potential vulnerabilities, more resources needed for protecting them and more opportunities to miss potential risks.

“As the data continues to grow exponentially, there’s going to be a much larger requirement for involving automation to find possible insider threats,” Doyle said. “Relying on humans to combat insider threats is not going to cut it. The automation and cognition sides of it are something that organizations are going to have to grow into.”

Artificial intelligence (AI) is an emerging technology that can automate data analytics, producing actionable insights from oceans of information. It can also reduce costs by eliminating many manual processes, freeing up resources for alternative spending elsewhere. Most importantly, AI reduces the burden on humans, helping them best focus their energies.

“Future insider threat protection will have a significant artificial intelligence capability,” McLaughlin said. “The solution needs to move at the speed of light.”

Pairing AI with other technologies like behavior analytics would produce a formidable force against insider threats.

“We’re going to be using integrated behavior anomaly detection to take inputs from access controls, server activity logs, privileged users and firewalls if they still exist in the future,” he said. “We’re going to be using AI to arrive at the conclusions. It’s a hub and spoke that’s going to be collecting the data and pre-filtering it.”

IBM’s AI tools strive to boost human defenses, increasing the speed with which they detect, investigate and react to insider threats while reducing costs.

“We’re using machine speed and cognitive capabilities to augment humans,” McMillan said. “Not to replace them, but to augment.”

How IBM Helps

The federal government's insider threats range from agency employees who accidentally expose sensitive data to disgruntled contractors intentionally causing harm. Effectively mitigating insider threats requires multiple tools for finding, stopping and preventing them.

Robust insider threat deterrence starts with strong data security. Solutions like IBM Security's Guardium family of tools keeps an organization's most valuable information shielded, preserving its public credibility and brand value. Tight data security also defends against costly interruptions and financial losses related to fraud and sabotage from insider threats. IBM provides tools for data encryption, control and vigilance alongside assigning and managing user privileges.

The next step is identity management. Answers like IBM's Access and Identity Management Services help agencies map the access pathways to their most critical data. Crucial information is assigned appropriate access controls, letting organizations determine who accesses it and how. Agencies can also govern their users' access privileges, dividing top officials from rank-and-file workers.

Behavior analytics help agencies proactively counter insider threats. Tools like IBM's QRadar User Behavior Analytics (UBA) detect the existence of malicious individuals and compromised user credentials. QRadar UBA establishes a baseline of daily enterprise activity, giving officials context for unusual behavior emerging from network, log, threat and vulnerability dangers. Security analysts see risky users more easily by observing potentially suspicious activities, flow and log data. This vigilance helps prevent attacks before they occur and stop existing ones before they cause further damage.

AI is the latest revolution in insider threat defense, helping analysts respond faster and more confidently. Manual activities are automated, reducing the time investment from humans. AI defenders skim increasingly large data sets, finding patterns with inhuman quickness. Tools like Watson, IBM's cognitive AI, get stronger and smarter from information patterns over time. Analysts then receive actionable insights for defeating insider threats more rapidly.

> *"We're using machine speed and cognitive capabilities to augment humans. Not to replace them, but to augment."*
>
> — Tim McMillan, Executive Security Strategist

Conclusion

Insider threats are a worst-case scenario for the federal government, as individuals can damage the entire whole.

All agencies are vulnerable to insider threats, which can emerge from carelessness and malice alike. This distinction lacks a difference for organizations that suffer embarrassment, damaged credibility and sensitive information exposure from insider threats. Some insider threats are unintentional, and some are never discovered.

Data security and asset and identity management provide a firm foundation for reducing insider threats. Newer technologies like behavior analytics and AI will take federal defenses against insider threats to the next level by augmenting human skills with machine speed.

“Five to 10 years from now, as the data continues to grow, there’s definitely going to be a larger requirement for involving more automation and orchestration to find a possible insider threat,” Doyle said.

About IBM

We confront the world’s most challenging cybersecurity problems and passionately protect the faces behind the data – your citizens. Through the intersection of AI, intelligent orchestration, the agility of the cloud, and collaboration with each other, we can tackle the cybersecurity challenges ahead of us.

For more information, visit us at www.ibm.com/federal/cybersecurity

About GovLoop

GovLoop’s mission is to “connect government to improve government.” We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 270,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop