Insider Threats: Mitigating the Risks at Your Agency

MARKET TRENDS REPORT

Introduction

Insider threats rank among the federal government's gravest challenges. Their proximity to sensitive information endangers agencies even more than external hackers. The potential harm to victims includes corporate espionage, intellectual property theft and undermining national security.

The broad variety of insider threats makes understanding and stopping them problematic. Organizations are often unclear about what they are and the risk they present. This leaves agencies ill-equipped for mitigating insider threats, which are evolving and spreading as technology advances.

The common trait insider threats have is their access to an agency's internal data, IT infrastructures and security practices. Such threats include bad actors, mistakes and poorly secured devices with network access.

To understand more about these perils and how to prevent them, GovLoop partnered with Carahsoft, an IT solutions provider, and Micro Focus Government Solutions, an IT software provider dedicated to helping agencies protect mission-critical data throughout its lifecycle, for this report. The following pages explain the risk insider threats pose to agencies and the best ways to mitigate them.

42%

of federal cybersecurity professionals said their agencies are the target of cyber incidents perpetrated by insiders.

45%

of federal cybersecurity professionals said they don't have insider threat employee training programs.

71%

of senior federal IT security executives said their agencies have been breached.

3x

the number of breaches were reported by senior federal IT security executives in 2017 than in 2016.

THE CHALLENGE

Facing Insider Threats from All Directions

Whether they're malicious attacks, information misuse accidents or poorly secured devices within your network, insider threats can emerge from anywhere in your organization, and the stakes surrounding insider threats couldn't be higher.

"The National Institute for Standards and Technology defines insider threats as the threat that an insider will use authorized access to do harm to the national security of the U.S., either wittingly or unwittingly," said Kevin Hansen, Chief Technologist at Micro Focus Government Solutions.

The most dangerous insider threats come from people, motivated by hostility toward the target, who weaponize an agency's sensitive information.

"They're knowingly and deliberately trying to cause damage," Hansen said. "It's espionage, fraud or a state actor looking for a competitive advantage over the U.S."

Accidental insider threats are different. They're the result of actions by people who may not know that what they're doing poses a security risk. It's an inconsequential distinction for agencies left picking up the pieces after an incident, however.

"Most of the advanced and persistent threats over the last few years have involved an inside user's stolen credential," Hansen said. "In most cases, that user was probably unaware that their credential was being used."

Privileged insiders are the riskiest threat, as they have special user access rights to sensitive organizational data, applications and systems. They typically aren't attempting anything malicious, but their privileges can make any security mistake on their part – or an attack targeting them – catastrophic.

"They inherently introduce a high-risk threat to the organization that you can't eliminate," Hansen said.

Agencies' woes will only grow as more devices connect to their networks. Left unsecured, these tools present as serious a danger as people.

Internet of Things (IoT) technology will only exacerbate this problem as more devices become capable of connecting to networks. Each new connection puts more pressure on agencies to defend their cybersecurity. This strains workforces already balancing cloud and legacy infrastructure cybersecurity.

The wide variety of insider threats means there are more chances for organizations to be caught off guard. Mitigating them requires juggling large amounts of agency network data.

"Agencies are having a hard time making sense of all the information that they're collecting," Hansen said. "They need to be able to identify what relationships exist between users, their roles and what groups they belong to."

Agencies lack visibility into their entire enterprise and understanding of the data it generates. They need a solution that collects and clarifies their vast amounts of information and creates actionable insights.

> *"Agencies are having a hard time making sense of all the information that they're collecting. They need to be able to identify what relationships exist between users, their roles and what groups they belong to."*
>
> – Kevin Hansen, Chief Technologist, Micro Focus Government Solutions

THE SOLUTION
Layered Security

Agencies should adopt a layered security approach that combines access, identity and security event management to detect and disrupt insider threats before damage is done.

This approach starts with multifactor authentication (MFA). MFA requires users to present two or more pieces of evidence about their identity before they can access sensitive data.

“Passwords are easy to steal historically and introduce a lot of risk,” Hansen said. “MFA relies on something that the user physically has and something they know. It increases the assurance of who that user actually is on your network.”

Once you’ve identified who is on your network, the next step is managing user access privileges. By determining which users can access which data, agencies ensure that no one has unnecessary access. They also establish normal user behavior patterns, making potential threats more visible.

“As a person evolves over time and changes roles, their permissions need to change as well,” Hansen said. “They may come in as a system administrator and become management down the road, and they no longer need those elevated permissions on those systems. That’s forgotten too often, and de-provisioning those permissions doesn’t happen.”

Alongside access privileges, agencies will also need to better manage their users’ behavior and identifying characteristics. This gives organizations the insights they need to understand who its users are, how they typically act and what they need to access.

To get even greater benefits from layered security, agencies can add machine learning and predictive analytics. These technologies boost the speed at which data can be analyzed for patterns and potential dangers. Predictive analytics examines current and past information to predict future outcomes, while machine learning involves computers “learning” from data to improve their performance on tasks without explicit programming.

Delivering these tools via automated methods helps agencies reduce the strain on their employees and better allocate their resources. It also frees up time for workforce training on how to avoid unintentionally becoming an insider threat.

“You want quick integration that increases your time to value on mitigating insider threats,” Hansen said. “If that integration’s going to be cumbersome, you should absolutely evaluate that.”

BEST PRACTICES

1. Reduce Access for Administrators and Other Privileged Users

Hackers frequently target IT and system administrators because of their broad network privileges. Limiting those employees’ access so that they cannot go everywhere reduces their risk to the organization. If they need access to a sensitive system, grant it to them temporarily and track it.

Reducing an organization’s number of privileged users also shrinks the potential for insider threat incidents. Fewer privileged users means fewer targets for cyberthreats and opportunities for accidents.

2. Gradually Apply These Tactics to Your Whole Agency

Users don’t need every system opened to them. Granting temporary, as-needed data access avoids insider threat exposure. Agencies should continuously monitor privileged users, however, because of the bigger risk. Contractors, branch office employees and “trusted” partners are additional examples of entities that can morph into insider threats with too much access.

3. Deploy the Right Tools

Using legacy tools to stop insider threats is risky, almost as risky as adding new, complex security features to legacy security infrastructures. A better solution is a platform providing integrated cybersecurity. It uses automation to control user access, monitor changes to critical systems and assets and provide security teams the context they need to spot and disrupt insider threats.

How CDM Improves Federal Cybersecurity

Agencies struggling with cybersecurity are turning to the federal government's Continuous Diagnostics and Mitigation (CDM) program.

The Homeland Security Department (DHS), in partnership with the General Services Administration (GSA), launched CDM in 2013. The program is a risk-based approach to cybersecurity that helps federal agencies fortify their networks and systems against potential threats. Agencies install sensors to perform automated, ongoing searches for known flaws and evidence of real-time or past attacks. The result is network managers who are more aware of the most critical cybersecurity risks, which enables them to allocate resources for handling them based on severity.

DHS announced in October 2018 that it was changing its language regarding CDM to focus on the program's capabilities rather than its phases. The goal is to get agencies thinking of asset management as a continuous effort rather than a task with a defined beginning and end. Nonetheless, understanding CDM's four phases is essential for maximizing the program's defensive abilities.

Phase I – What is on the Network?

This step requires the management and control of agencies' devices, software, security configuration settings and software vulnerabilities.

Phase 2 – Who is on the Network?

This stage mandates the management and control of accounts, access and managed privileges. Phase 2 also requires determining which users get what access, credentials and authentication and security-related behavioral training. These various functions are interdependent, and Phase 2 ultimately manages them together.

Phase 3 – What is Happening on the Network?

This phase is critical for dealing with problems such as insider threats as it moves agencies' capabilities from asset management to more extensive, dynamic monitoring of security controls. This shift includes preparing for and responding to behavior incidents and ensuring that software and system quality are integrated into agencies' networks and infrastructure. Phase 3 also detects internal actions and behavior to determine who's doing what at organizations and focuses on protecting data at rest and in transit. Additionally, this phase mitigates security incidents to prevent them from spreading throughout agencies' networks and infrastructures.

Phase 4 – How is Data Protected?

This segment continuously identifies cybersecurity risks, prioritizes each one based on the potential impact and enables personnel to mitigate the most significant dangers first.

Working together, CDM's phases help agencies monitor and mitigate cyber risks in real time. This ongoing vigilance makes both the federal government and the citizens it serves safer in an increasingly hostile threat landscape.

How Micro Focus Government Solutions and Carahsoft Help

Micro Focus' broad and integrated security platform combines asset management, identity and access governance (including privileged account management), data classification and governance and security event management to provide the full range of organizational knowledge around who users are, what activity is normal for them and what they need access to. Typical security suites provide only one or two of these capabilities, leaving agencies to manually integrate and correlate data among the various third-party systems, whereas the Micro Focus platform gives security teams greater visibility and context into what is happening on their network much faster. This not only helps agencies realize security compliance quickly, but more importantly identify activity that poses a threat and use governing controls to automate mitigation of those threats, minimizing the associated risks and exposure time more quickly.

"Micro Focus and Carahsoft are purpose-built and mission-driven on this issue," Hansen said. "Our products are available on GSA's CDM Schedule 70 and are currently protecting agencies against insider threats."

The Micro Focus security platform provides unmatched integration to address CDM program requirements including:

Phase I

What's on the network?

- Unified Endpoint Management
- Secure Configuration Management

Phase 2

Who is on the network?

- Identity and Access Management
- Privileged Account Management
- Directory Resource Management
- Advanced Multifactor Authentication

Phase 3

What is happening on the network?

- Identity and Access Governance
- Security Operations
- Secure Application Development

Phase 4

How is data protected?

- Information Management and Governance
- Data Protection

"Critically important, we're helping agencies aggregate all their user identity information," Hansen said. "It's about creating a central identity vault that can be leveraged to manage user permissions, identity attributes and feed more actionable insider information into security event management systems."

Conclusion

There's no cure for insider threats, but the right mix of tactics and technology can find and mitigate them faster. A platform that simplifies agencies' access, user and security event information is a must. MFA is a powerful countermeasure, while predictive analytics and machine learning help organizations take preventative measures. Integrating these practical steps in compliance with federal regulations soothes the headaches insider threats give agencies.

Federal workers are the last line of defense against insider threats. Employees who recognize what insider threats are and how they operate can limit them.

"The federal government's cybersecurity and insider threat training has really improved and been more effective," Hansen said. "Having a better-informed workforce is a big step forward when it comes to protecting against these unknown threats that exist, but there's still a fair amount of work to do."

ABOUT MICRO FOCUS

Micro Focus Government Solutions is a purpose-built, mission focused company that serves US public sector clients. A company anchored by success in the IT industry, Micro Focus Government Solutions is uniquely positioned to help your organization bridge the gap between legacy systems and modern innovation. Backed by one of the largest pure-play software companies in the world, Micro Focus, we help solve critical IT challenges with software solutions in Hybrid IT, DevOps, Security & Risk, and Predictive Analytics.

Learn more at www.microfocusgov.com

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 300,000 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

govloop

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

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

www.govloop.com
@GovLoop