Watch Your Back: How to Prevent Insider Threats

By Matthew Garlipp, GovLoop

Edward Snowden. Robert Hanssen. Bradley Manning. Aldrich Ames. At one point, these people were all part of workforces that organizations depended on. But an organization's backbone can soon become its biggest vulnerability. With insider threat costs ranging from $5,000 to $3 million per incident, how can your agency address the potentially devastating impact of an insider threat? Roy Gingher, Technical Account Manager, Symantec, and Kevin McPeak, Technical Architect, Security: Public Sector Strategic Programs, Symantec, provide valuable insight into the profile of insider threats, the challenges they pose and how Symantec can help your agency prevent them from occurring.

What are insider threats?

In examining insider threats, Gingher provided a definition he often uses:

> "An insider threat arises when a person with authorized access to U.S. government resources through facilities, information, equipment, network and systems, uses that access to harm the security of the U.S. Malicious insiders can inflict incalculable damage and enable the enemy to compromise our nation's most important endeavors."

To gain a better understanding of this threat, it's also helpful to examine the perpetrators, themselves.

Profile of an Insider Threat

Non-Malicious

An important thing to consider is that insider threats aren't just malicious people. "The insider threat is an overworked administrator that forgets to take permissions away from somebody and somebody Has access to something he shouldn't," said Gingher.

"Not everyone who is an insider threat does harm with malicious intent," echoed McPeak. "A lot of our federal workforce is under tremendous pressure to get their mission done. It's an increasingly complex world that we live in, with progressively complex challenges that our nation faces, often with dwindling resources." This pressure may lead to costly mistakes. McPeak explained further:

"In order to get the job done quickly, they might want to copy and paste [file/project information] from one file share structure to another, or from one server, one network architecture over to another, even cross classification boundaries. They may want to do something like that in the spirit of getting the mission done, but what they end up doing is

compromising the integrity of the system. So, their heart may have been in the right place, but they violated policy which led to a data spill or some type of an exfiltration."

Malicious

Sometimes, however, the intent is malicious. Motives may involve extreme ideology or financial gain but could also be strongly correlated to personality type. "One theme that, at least in recent history, seems to pop up quite a bit is a personality characteristic where the person has a lot of issues around their own self-esteem and their own sense of self-worth," said McPeak. An insider may feel his voice goes unheard, and he may be frustrated by his lack of influence in the organization. On the other hand, an insider may be overconfident and arrogant and proactively seek out opportunities to steal and spill sensitive data.

System Administrators

Possibly the most dangerous type of insider that can inflict incalculable damage is a system administrator. These insiders have "god-like" access to an organization's information, with physical and logical access and elevated rights across most of its systems. "They can burn the house down, so to speak, in a matter of minutes if they have that much access," said McPeak. According to Symantec, 86 percent of insiders stole data from an area they were directly involved in and 75 percent stole material they had authorized access to.

Preventing Insider Threats Best Practices

Data Classification & Prioritization

An effective way to halt an insider threat is data classification and prioritization. Through "data tagging," you can secure your most important information at a higher level, explained Gingher. You can also separate data ensuring that if an insider does strike, the information will not be in the aggregate. Separation of duties to prevent "god-like" access across platforms is also critical. "Properly identifying and tagging your sensitive data is key to this effort," said McPeak. "A lot of times an organization might think sensitive data lives on a certain server but specific users might be copying it to another location," he continued. "They could be saving it to their local desktops, so there's a lot of ways that the data can move around and morph."

Training

Having employees better understand insider threats is crucial. "If you have your people trained right, they understand that if you don't complete the loop – if you don't lock down the document, or mark it right – you're helping an insider do their job easier," said Gingher. Prioritizing deterrence over detection is important since "the biggest threat is the worker that makes a mistake," he said. Knowing what to look for is also crucial. "If you see something, say something," advised McPeak. "If somebody's behaving suspiciously or making negative statements about management, there should be channels in place for you to tip that off."

A Balancing Act

You want your organization to be secure, but not overly burdened with costly requirements. As your security complexity increases, that calls for IT staff and other expensive requirements. "It's about hitting the right balance of total cost of ownership of

your operations and maintenance to have all of those diversified positions," McPeak explained.

How Symantec Can Help

In addition to data classification and prioritization, Symantec's data loss prevention (DLP) solutions can help impede insider threats in multiple ways. "We have the ability to go into a network and know who's touched every file, when it was touched, how old the file is, who owns the file," said Gingher. "By knowing that, we can then build a social network of your data inside your organization and see people which we call 'outliers.' People that should not have permission to touch things, but that do."

Symantec's software can also automate access to prevent inadvertent, costly mistakes. Unauthorized data access or movement is disallowed with pop-up warnings or by having that action bounced up to a management level for approval. Other services include monitoring for email sent to iOS devices, the ability to evaluate encrypted content for policy violations, and greater visibility into the behavior patterns of high-risk insiders.

On one hand, employers are the life-blood of organizations. On the other, they pose the biggest risk to their success and longevity. Accordingly, the importance of protecting your agency from insider threats cannot be overstated. Training, awareness, and solutions from vendors such as Symantec can help ensure this protection and, thus, the welfare of your agency.