VIRESCIT TACTICAL SYSTEMS

A WHOLLY OWNED SUBSIDIARY OF WiSC ENTERPRISES

"Make Cybersecurity valuable, achievable, and engaging."

INSIDER THREAT

by Jason Lorenz, VTS Program Services Coordinator

INTRODUCTION

Companies all over the world and throughout the United States suffer massive costs from insider threat by people in positions of trust. These individuals have the potential to misuse access knowingly or unknowingly to networks within an organization. Insiders or individuals within an organization have caused more damage to the organization itself than known outside threats.

The Department of Defense (DoD) Counterintelligence and Security Agency (DCSA)[1] defines insider threat as: Acts of commission or omission by an insider who intentionally or unintentionally compromises or potentially compromises DoD's ability to accomplish its mission. While this definition is applied to the DoD, it's the same damage to other agencies and private companies which harms finance, trust, and security throughout the world.

The DCSA definition includes two parts of note:
First, the threat is an individual (or group) human being, emphasizing that insider threat is a *human* problem. Second, witting or unwitting events, actions or neglect all pose danger.

We will describe five types of insider threats with the potential to damage an organization. More importantly, vulnerabilities within your organization and how to protect your organization from insider threats, along with responses and how to report a suspected insider threat.[2]

EXAMPLES OF INSIDER THREAT

In the white paper, "Categories of Insider Threat," The Intelligence National Security Alliance (INSA)[3] describes five types of insider threat activity which will severely damage an organization's interests:

Sabotage

An insider's destruction of electronic or physical property intended specifically to harm his/her own organization.

Theft

An insider's theft of intellectual property, data, or classified information relevant to national security. This category encompasses the traditional concept of espionage as defined by applicable statutes.

Fraud

Modification, addition, deletion, or inappropriate use of an organization's information, data, or systems for personal gain. Examples include insider trading, embezzlement, and other actions to defraud the organization by an employee, contractor, or trusted business partner.

Unintentional

An insider who has or had authorized access to the organization's network, system, physical facility, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems. Examples include accidental public disclosures of sensitive information, phishing scams, and loss of organizational records and/or electronic media.

[1] https://www.dcsa.mil/
[2] https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf
[3] https://www.insaonline.org/wp-content/uploads/2019/10/INSA_WP_Categories_of_Insider_Threats-1.pdf

Workplace Violence
Any act or threat or act of physical violence, harassment, hazing, intimidation, or other threatening disruptive behavior that occurs at the work site.

INDICATORS AND REPORTING

Malicious insiders tend to have leading indicators. Focus on monitoring employees that display these high-risk behaviors. Here's what to watch out for:

Poor Performance Apraisals
An employee might take a poor performance review very sourly. In 2012, Ricky Joe Mitchell, a former network engineer at an energy company, learned that he was going to be fired and intentionally sabotaged his company's computer system, leaving them unable to fully communicate or conduct business operations for about 30 days.

Voicing Disagreement with Policies
Someone who is highly vocal about how much they dislike company policies could be a potential insider threat. They may want to get revenge or change policies through extreme measures. Employees have been known to hold network access or company data hostage until they get what they want. In 2008, Terry Childs was charged with hijacking his employers' network. He was arrested for refusing to hand over passwords to the network system that he had illegally taken control over.

Disagreements with Coworkers
Look out for employees who have angry or even violent disagreements with their coworkers, especially if those disagreements are with their managers or executive staff.

Financial Distress
An employee who is under extreme financial distress might decide to sell your organization's sensitive data to outside parties to make up for debt or steal customers' personal information for identity and tax fraud.

Unexplained Financial Gain
Watch out for employees who have suspicious financial gain or who begin to buy things they cannot afford on their household income. If someone who normally drives an old beat-up car to work every day suddenly shows up in a brand new Ferrari, you might want to investigate where the money is coming from, especially if they have access to expensive and sensitive data.

Odd Working Hours
Pay attention to employees who normally work 9-5 but start logging in or accessing the network later or outside the usual hours of their peer group without authorization or a true need to work outside of normal hours.

Unusual Overseas Travel
Unusual travel to foreign countries could be a sign of corporate or foreign espionage. Especially, travel not required for work, to a country in which they have no relatives or friends, or a place not typically a tourist destination. Sometimes, however, travel can be well-disguised. For example, convicted spy Greg Chung spied for China for nearly 30 years and said he was traveling to China to give lectures. Instead, he was stealing hundreds of thousands of documents from his employer and meeting with Chinese agents. Look for unexpected or frequent travel that is accompanied with the other early indicators.

Leaving the Company

Anyone leaving the company could become an insider threat. When someone gives their notice, examine the past 90 days of activity and see if they've done anything unusual, inappropriate, or accessed data they shouldn't have.[4]

ORGANIZATIONAL VULNERABILITIES

Joseph Carson, chief security scientist and advisory chief information security officer at Thycotic, told Threatpost: "The [work from home] trend due to the COVID-19 pandemic has significantly increased insider threats from employees taking risks with company assets, such as stealing sensitive data for personal use or gain as employers have less visibility to what employees are doing or accessing".[5]

With issues such as the COVID-19 pandemic, in a broader connected world, more organizations face danger from insider threat. Does your organization issue computers or the equipment needed to operate effectively from home? Are there policies or restrictions implemented on company equipment to monitor or restrict relevant company information? These are just two questions that we as leaders within an organization need to consider to limit the possibility of insider threat.

CONCLUSION

While insider threat has continuously been a problem for countless organizations for many years, recent reports have shown an increase concerning insider threat. Throughout 2020, many companies have been disproportionately affected by COVID-19. Because of this, cloud networking and telework (working from home) has expanded, which results in less control of our organizations critical data and information systems. Important information concerning your organization is far more easily "leaked" and can quite possibly be harder to track. Individuals, communication, and clear policies that are easy to understand can help teams to ensure our organization does not fail due to insider threat.

Our mission at Virescit Tactical Systems (VTS) is to "make Cybersecurity valuable, achievable, and engaging". Our team is composed of dedicated professionals that can provide you with the skills, training and policies needed to ensure your organization is protected, not only from external threats, but insider threats as well.

[4] https://digitalguardian.com/blog/early-indicators-insider-threat
[5] https://threatpost.com/work-from-home-opens-new-remote-insider-threats/156841/

[13] https://vtscyber.com/training-certification/

[14] https://www.nist.gov/cyberframework/new-framework

[15] https://csrc.nist.gov/projects/risk-management/rmf-overview

[16] https://csrc.nist.gov/publications/detail/sp/800-207/final

[17] https://www.zdnet.com/article/what-is-cyber-insurance-everything-you-need-to-know-about-what-it-covers-and-how-it-works/

[18] https://us-cert.cisa.gov/ncas/alerts/TA15-119A