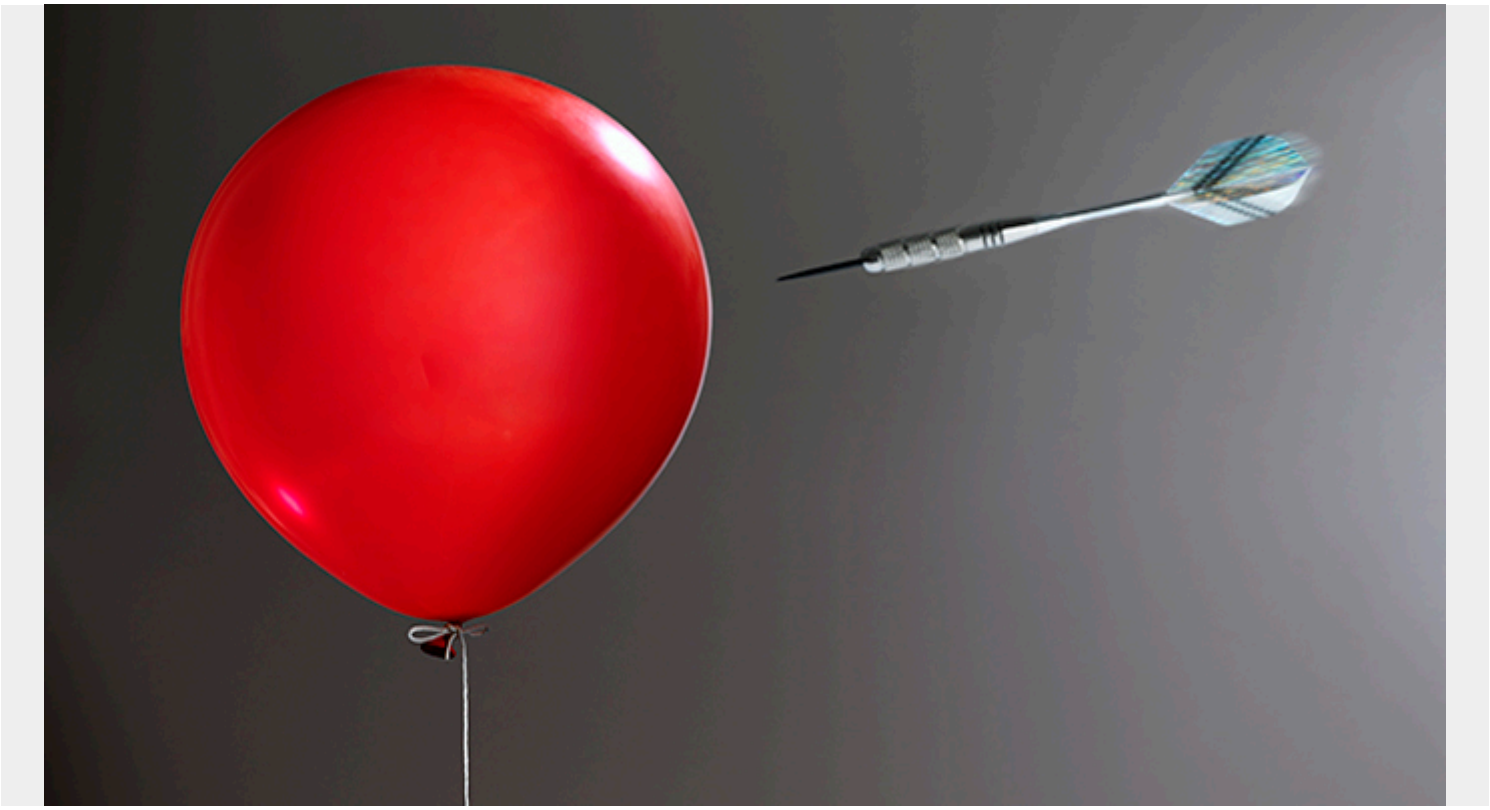
INSIDER THREATS: THE GOOD, THE BAD, AND THE UGLY



Wikipedia describes an insider threat as *"a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems."*

CERT redefined "insider threat" in March 2017 to cover malicious and non-malicious (unintentional) insider threats; to also include both cyber and physical impacts; and to apply the new definition to both government and industry. CERT's main goal entailed making the term "insider threat" clear, concise, and consistent with existing definitions of 'threat' and broad enough to cover all insider threats.

CERT achieved their goal with this succinct definition:

"Insider threat — the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization."

For the purpose of this blog post, let's flow with CERT's definition.

The good

Earlier this year The Institute for Critical Infrastructure Technology (ICIT) published a gripping report

on insider threats. This fascinating report filled with "think tank" objectives, detailed comprehensive insider threat categories and other innovative ideas that I had not considered prior to reading this report—like company culture and the human factor as capable of maintaining both the strongest and weakest link in every organization's cybersecurity.

"At their core, organizations depend on trusted personnel to access critical systems, to make pivotal decisions, and to carry out vital operations. Despite all the technological innovation of the digital age, humans remain the strongest and the weakest link in every organization's cybersecurity." —ICIT

The good news about insider threats is the fact that the security world is beginning to take notice:

"Insider Threat is still fairly new to organizations and the awareness of the problem is just emerging today." —Michael Crouse, Forcepoint Director Federal Technical Sales & ICIT Fellow

Though holistic insider threat awareness programs (CERT, PhishMe, SANs) and sophisticated security technologies and advanced tools (predictive AI, DLP, machine learning, SIEM, UAM, UEBA) are available, adoption is still in its infancy.

Since perimeter-based defenses are incapable of mitigating insider threats, companies will need to up their IT budget and invest in advanced security tools and technologies that are tailored specifically for their network infrastructure.

The bad

According to the 2017 Verizon Data Breach Investigations Report (DBIR), in 60 percent of insider threat cases, insiders absconded with data in hopes of converting it to cash in the future. Also, 17 percent involved unsanctioned snooping and for the remaining 15 percent, the insider either took data to a new employer or started a rival company.

The Harvey Nash/KPMG Survey of 4,500 CIOs and technology leaders from around the world (surveyed between December 2016 and April 2017) found that more people are reporting trouble from "insiders".

All these recent reports and surveys paint a grim portrait of what continues to hover on the threat landscape this year. *"Everyone operating in critical infrastructure sectors has heard of insider threats ranging from Julius and Ethel Rosenberg to Robert Hanssen; however, insiders develop and operate differently in the digital age,"* says ICIT. Further elaborating: *"Insider threats do not have to be well-positioned, hackers, or technologically sophisticated to inflict catastrophic harm on critical infrastructures or average Americans. No matter how many organizational resources are exerted, humans remain the one data container that employers cannot secure."*

If this holds true and employers can't secure their employees from becoming an insider threat—what's next?

With minimal recognition of insider threat problems, many organizations will continue to grapple with data breaches and under-trained staff who practice bad cyber-hygiene. Oftentimes, many companies fail to fully implement "mature" cybersecurity training and awareness programs. Many of these training programs are too long, too hard, and exceptionally boring—with the end result being cognitive overload.

The ugly

If we go back in history—it's taken way too long for organizations to beef up perimeter defenses to keep up with the external threat landscape. How long will it take for organizations to bolster and fortify their network infrastructure to address and mitigate insider threats?

Another area of grave concern that often slips through the cracks is the dark web—replete with cybercriminal markets that provide new and intriguing playgrounds for disgruntled employees. At Gartner's recent Security and Risk Management Summit, analyst Avivah Litan said *"Corporate employees who help carry out cyberattacks are increasingly being sought and are seeking criminals to hire them."*

ICIT concluded their report with this somber warning:

"Insider threats begin with trusted employees whose frustration, resentment, apathy, lack of cybersecurity training and awareness, or external motivations radicalize them to unintentionally or willfully inflict harm on the organization by compromising systems, assisting external cyber-threat actors in multi-vector information warfare, or exfiltrating treasure troves of valuable PII, PHI, and other sensitive data."

Lest we forget:

"Insider Threat is still fairly new to organizations and the awareness of the problem is just emerging today." —Michael Crouse, Forcepoint, Director Federal Technical Sales & ICIT Fellow

Visiting sites like Glassdoor which house myriad negative employee reviews—from start-ups to Fortune 500 companies—many list company culture as the major culprit of employee dissatisfaction and disillusionment. Some of the reviews that caught my eye include:

- *The company does not appreciate anyone and is condescending.*
- *Siloed teams and complete chaos.*
- *Marketing is disconnected from reality.*
- *Upper management protected their cronies and laid off employees with no warning or severance.*
- *Politics play a huge role in advancement.*
- *Monotonous and boring work. Too much micromanagement.*
- *Toxic culture where screaming at subordinates (who are not part of the "in" crowd) is the norm.*

I see the writing on the wall. Do you? Though the insider threat conundrum is still a baby that has not yet learned to walk—it is crawling. 2017 is the year that the *insider threat* baby may go beyond its first few steps and learn to walk. Take heed.

Main Source:

Scott, J., & Spaniel, D. (2017, February). In 2017, The Insider Threat Epidemic Begins. Retrieved June 12, 2017, from http://icitech.org/wp-content/uploads/2017/02/ICIT-Brief-In-2017-The-Insider-Threat-Epidemic-Begins.pdf