To Catch an Insider Thief

The scene played out in films is of a terrified victim learning that the menacing phone calls are coming from inside the house. The scenes in real-life organizations across the government and private sector are not that different. Information warfare and cyber security threats to national security are typically associated with Russia, China, or terror groups. However, the most daunting threats too often come not from outside adversaries, but from once trusted, but disloyal employees.

The rise of insider threats has made organizations across the private sector and government rethink their information and physical security. In a 2016 survey of enterprise security professionals, 69% indicated they had "experienced attempted or successful data theft or corruption by corporate insiders during the prior 12 months."[1] The national security community fares much worse. Bradley Manning's unauthorized access, retrieval, and disclosure of 750,000 pages of U.S. military and diplomatic reports, and other sensitive information in 2010 made WikiLeaks a household name. Last month WikiLeaks released thousands of purported CIA documents on extensive cyber-espionage tools and programs worldwide. Edward Snowden, who leaked classified information about global surveillance programs from the National Security Agency in 2013, tweeted from Russia about another NSA contractor, Harold T. Martin III, who was arrested by the FBI in 2016 for possession of potentially damaging top-secret information.

There is legitimate anxiety over the threat to organizations from their own people. The problem, however, isn't anything new. Information has always been a commodity. A 2016 Gartner survey found 62% of malicious insider incidents "involved employees looking to establish a second stream of income off of their employers' sensitive data, 29% stole information on the way out the door to help future endeavors and 9% were saboteurs."[2] The new twists to this problem are the speed, volume, reach, and impact of malicious insiders, which make identification, prevention and responsiveness that much harder. However, the problem isn't solely about the perpetrator. The human factors that lead insiders to compromise information and organizations are complicated by the all-too-human and organizational flaws of the targets themselves.

Complacency

Too many organizations seem to believe that security rules and processes are working, with little or no potential for insider threat problems. According to one survey, nearly one-third of all responding organizations had no capability to prevent or deter an insider incident or attack, while only 9% ranked their insider prevention methods as very effective.[3] The urgency to deal with potential insider threats often fails to materialize until the impact is real, with the average cost of incidents ranging from $200,000 to $500,000, plus the inestimable loss of information or life.[4]

---

[1] Accenture, "How to secure your customer's digital trust; Re-thinking 'State of the Art' in Cybersecurity," June 2016, https://www.accenture.com/us-en/insight-cybersecurity-digital-trust-2016.

[2] Ericka Chickowski, "8 Surprising Statistics About Insider Threats," *Dark Reading*, August 17, 2016, http://www.darkreading.com/vulnerabilities---threats/8-surprising-statistics-about-insider-threats/d/d-id/1326653?image_number=1.

[3] Ibid.

[4] Kim Lindros, "Stopping the Insider Threat: Securing Your Business from Employees," *Business News Daily*, March 9, 2017, http://www.businessnewsdaily.com/9806-insider-security-threats.html.

If an ounce of prevention is still worth a pound of cure, then organizations need to improve protections to deter and prevent insider threats, and develop a formalized ***InsiderSafe*** type of program.[5] The first step is upgrading and modernizing existing tools and infrastructure (hardware and software), regularly identifying and closing the holes. Management must also update practices, training, and standards, incorporating insider threat awareness into the organization's culture and stressing the importance of reporting insider threat activity to the appropriate security teams. The well-known "see something, say something" campaign has yet to permeate in organizations where reporting may not be available or is otherwise equated to snitching. One organizational accountability survey found that some two-thirds of employees saw a problem arising, but did nothing about it. Monitoring is certainly a subjective challenge. However, organizations must observe and respond to suspicious behavior, as well as anticipate and manage negative workplace issues. They can identify and prioritize those networks or programs that could be vulnerable to malicious insiders. Increased employee screening and physical security should be examined, as many thefts are accomplished the old-fashioned way; insiders simply walk out the door with the information. Customers and partner organizations should also be engaged to cooperatively address vulnerability issues.

Such improvements have proven to be effective. Since Snowden's disclosures, for example, the federal government has reduced the number of people who hold security clearances by 17%, while the quality of background checks has been enhanced.[6] In late 2016, the Pentagon's Defense Security Service required all contractors to implement programs that are designed "to detect, deter and mitigate insider threats" and to designate "a senior insider threat official to oversee the program and provide training on how best to implement it."[7] There is still a long way to go. Studies found that 62% of business users reported that they had access to company data that they believed they shouldn't see. Meanwhile 43% of businesses still needed a month or longer to detect employees' unauthorized access to files or emails.[8] One practical approach is implementing role-based access controls on automated systems to alert an organization's authorities if an insider tries to access information beyond what's needed to perform their role. It would appear that as long as organizations believe existing resources and processes are working, the risk of being the target of insider threats will only grow.

<u>Shortsightedness</u>

Taking steps toward thwarting insider threats is not a one-time exercise or a simple automatic update of a security program on a computer. Insider threat awareness and prevention requires ongoing, long-term process improvement and continuing investment. This need is exemplified by the federal personnel clearance process. The government's human-intensive background investigation process is unable to provide timely and effective reviews and updates for the backlog of applications for over half a million people. One suggestion is to "move expeditiously to a system that relies less on manual background investigations and increasingly on automated records checks, continuous evaluation, and artificial

[5] The U.S. Navy's CYBERSAFE, which provides maximum reasonable assurance of survivability and resiliency of mission critical IT and capabilities in a contested cyber environment, conceptually is an example of such a program.
[6] Tami Abdollah and Eric Tucker, "NSA contractor arrest highlights challenge of insider threat," *Associated Press*, October 6, 2016, http://ktvl.com/news/nation-world/nsa-contractor-arrest-highlights-challenge-of-insider-threat-10-06-2016-192925791.
[7] Christian Davenport, "NSA case highlights growing concerns over insider threats," *Washington Post*, October 6, 2016, https://www.washingtonpost.com/business/economy/nsa-case-highlights-growing-concerns-over-insider-threats/2016/10/06/61b90a5e-8bc7-11e6-bf8a-3d26847eeed4_story.html?utm_term=.c068131763e0.
[8] Ibid.

intelligence-enabled data analytics to monitor the reliability of people who hold classified security clearances and access our facilities across government and industry."[9] Automation can augment the investigation process to support the interpersonal investigation activities, but it *cannot* replace them.

Some insider threat mitigation processes and technologies are already showing promise. Digital watermarking "imprints digital documents with a watermark code that shows who accessed them and when, which would allow officials to track the documents and ultimately discourage leaks."[10] Organizations are increasingly being encouraged to develop digital playbooks that "identify the criteria for determining how an event qualifies as an insider threat, provide a checklist for actions to take, and lists the key company actors that must be involved, whether IT or security staff, leadership or third party providers."[11]They also identify processes that can be automated and assign resources to those areas more at risk. New insider threat tools also examine the most subjective aspect of the threat – human behavior. Behavior-based detection and analytics, as well as "advances in artificial intelligence and deep machine learning, will enhance our ability to hunt for anomalous or alarming behavior while further limiting the impacts on those in our community who are doing nothing wrong and focused on the mission."[12] There are still concerns about systems or processes being able to discern unusual behavior that signals malicious insider threats from simple human error or accidents. Employees should expect to be monitored when they step into their office or log on to the organization's network (particularly those with clearances). However, how far can organizations go when irregular remote access, lavish purchases, social media activity, or other suspicious behavior is detected? Cognitive computing is being explored by government agencies in efforts to continually monitor both programs and workforces. "By analyzing electronic communications, social media and web activity, along with human resources records, cognitive computing can help agencies spot erratic behavior and prevent insider threats before they become a problem."[13] Questions concerning the balance between increased monitoring capabilities and privacy laws also must be addressed.

While the technology side continues to evolve, one essential step is to develop a security plan for all new investments under consideration or implementation. "Every time you consider investing in a new capability or technological advantage, ask your team to also show you how it will be protected against adversaries who want to steal, copy, or reveal it. And hold one member of your senior team accountable for ensuring there is a comprehensive, enterprise-wide strategy in place."[14] Those who want to steal, be they criminals, insiders, or nation states, are typically believed to be one step ahead of those from whom they steal. Both the government and private sector need to turn the tables on insider threats or risk always being a step behind.

Denial

In 2001, the FBI arrested "the worst spy in U.S. history" who had been spying for the Soviet and Russian intelligence services since 1979. The triumph was diminished by the fact that they had gone after the

[9] Marcel Lettre, "I Ran Intel at the Pentagon. Here's My Advice on Insider Threats," *DefenseOne*, March 13, 2017, http://www.defenseone.com/ideas/2017/03/i-ran-intel-pentagon-heres-my-advice-insider-threats/136119/.
[10] Sean D. Carberry, "Vault 7 leak highlights insider threat," *FCW.com*, March 10, 2017, https://fcw.com/articles/2017/03/10/vault7-insider-threat-carberry.aspx.
[11] Robert N. Rose, "The Future Of Insider Threats," *Forbes*, August 30, 2016, https://www.forbes.com/sites/realspin/2016/08/30/the-future-of-insider-threats/#5e65dde27dcb.
[12]Lettre, op.cit.
[13] Francesca El-Attrash, "Humanizing the Way Government Tackles Insider Threats With Cognitive Computing," *govloop*, March 10, 2017, https://www.govloop.com/resources/humanizing-way-government-tackles-insider-threats-cognitive-computing/.
[14]Lettre, op.cit.

wrong person for years. The FBI had focused on an undercover CIA officer who had broken other spy cases and passed several tests of innocence while under investigation. What happened? The investigation was sometimes misdirected by the real spy, Robert Hanssen, an FBI agent. Clues pointed to a mole within the FBI as early as 1999 and even to Hanssen, whose lifestyle and finances were suspicious. However, many key FBI officials couldn't believe the possibility of an inside man. "If there was a spy in the FBI that was an admission that we were flawed."[15] Entrenched organizational and cognitive biases can be as problematic as the insider threat itself and often contribute to the damage done. "Observations and events are filtered through a prism of culture, assumptions, biases, and experiences, leading actors to mistake the unfamiliar with the improbable."[16]

Denial also makes an organization predictable. Cold War-era KGB agent Yuri Totrov identified 26 unchanging indicators for identifying U.S. intelligence officers overseas, such as placing CIA officers in the same embassy posts, driving the same kind of car, and renting the same apartment.[17] Today thousands of factors can be monitored and patterns spotted in near real-time through big-data analytics. Organizations must accept that their known processes and technologies can be used against them. Studies of insider IT sabotage found "that the insiders overwhelmingly took advantage of their knowledge of the IT security systems, creating access pathways for themselves completely unknown to the organization… they invented ways to attack that the security planners had not known were possible."[18] Acknowledging the possibility that an insider threat even exists disturbs an organization's reality, and denial becomes a self-defense mechanism. No threat can be prevented or mitigated when the threatened can't see, can't accept, or can't manage the situation.

While no organization can be 100% safe, insider threats increasingly remind organizations that they are always vulnerable. With the growth of Internet of Things devices, attacks and breaches will also take on new forms. Whatever the motive or tool, it can't be denied that insider knowledge certainly provides the means. Individual integrity and character are difficult to assess and monitor. The insider threat problem requires leaders to make it a top priority, creating a program of sustained vigilance throughout their enterprises that integrates behavioral approaches with effective personnel security and counterintelligence processes. They must also "recognize the importance of leveraging innovative technology and data sources to monitor and evaluate individuals on a continuous basis."[19] While the problem may not be totally eliminated, the means to greatly reduce the severity and impact do exist. Organizations must look at their own culture, beliefs and behaviors as a fundamental measure of protection from threats and ensure that they are constantly and consciously re-examined. Otherwise, they will face the consequences when the call says that the attack and security breach came from the inside.

---

[15] Mary-Jayne McKay, "To Catch a Spy; Probe to Unmask Hanssen Almost Ruined Kelley," *CBS News*, January 30, 2003, http://www.cbsnews.com/news/to-catch-a-spy-30-01-2003/.

[16] "Decision Superiority: Countering Surprise, Denial, and Deception," September 2012, https://www.asymmetricthreat.net/docs/AsymThreat_WP6.pdf.

[17] Jonathan Haslam, "How to explain the KGB's amazing success identifying CIA agents in the field?" *Salon*, September 26, 2015, http://www.salon.com/2015/09/26/how_to_explain_the_kgbs_amazing_success_identifying_cia_agents_in_the_field/.

[18] "A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes," American Academy of Arts & Sciences, 2013, https://www.amacad.org/content/publications/pubContent.aspx?d=1427.

[19] "Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytics to Improve Continuous Evaluation," Intelligence and National Security Alliance, April 2017, http://www.insaonline.org/i/d/a/b/MindofInsider_wp.aspx.