SECURITY
MANAGEMENT

Protecting Your Company from Insider Threats

A collection of articles on emerging threats and practical solutions from the security industry's premier publication.

Powered by

ASIS INTERNATIONAL

Advancing Security Worldwide®

SECURITY
MANAGEMENT

ASIS INTERNATIONAL
Advancing Security Worldwide®

Security Management is the award-winning publication of ASIS International, the preeminent international organization for security professionals. *Security Management* is written primarily for security professionals. It also makes vital security information understandable to a general business audience, helping ASIS International advance security worldwide. Readers receive timely information on emerging security threats and practical solutions, which they can use to protect people, property, and information.

To join ASIS International and become a subscriber to *Security Management*, visit asisonline.org/membership/join.

Copyright © 2020 *Security Management*. All rights reserved. 2020 *Security Management* is an affiliate of ASIS International. The content in this document may not be reproduced, distributed, transmitted, cached or otherwise used, except with prior written permission of *Security Management*, ASIS International.

SECURITY MANAGEMENT

Leveraging Public Data to Mitigate Insider Threats

Worrisome indicators often precede insider threats. More and more, these indicators are reflected in publicly available spaces.

By Val LeTellier

Insider attacks generally take the form of theft, fraud, sabotage, or violence by individuals with access to the critical resources of an organization. Unsurprisingly, worrisome indicators often exist prior to these malicious acts. More and more, these indicators are reflected in publicly available spaces.

For example, before the 5 December 2019 attack at Pensacola Naval Air Station in Florida, Saudi Air Force officer Mohammad al-Shamrani exhibited anomalous behavior. He obtained a Florida hunting license and bought a handgun and several extended magazines—not common hunting gear.

Al-Shamrani then began making increasingly extreme social media posts. Hours before the attack that left three U.S. Navy sailors dead, he posted a hate-fueled manifesto on Twitter. A post-incident investigation found that 17 of al-Shamrani's fellow Saudi students had social media pro-

files containing jihadi or anti-American content. More than 12 Saudi servicemen were expelled from the United States after a Pentagon-ordered review of the program.

Like many before it, this attack raised the question of how public data can be leveraged to detect and prevent insider attacks. But why should organizations consider using publicly available information to safeguard their people, property, and profit?

There are three main reasons: insiders tend to not act impulsively but move slowly toward action; they leave clues in their progression along the insider kill chain in the form of changes in attitude and behavior; and these clues are increasingly found in public data.

Driven by the growth of the Internet and ubiquitous personal and professional use of mobile devices, availability of public data has exploded. Detailed personal, financial, and professional data can be found on almost anyone. The increasing strength and availability of data analytical tools means that massive amounts of personal data can be instantly aggregated, profiled, and made publicly available.
This expanding digital domain is complemented by widespread use of social media platforms. The public forums of Facebook, Twitter, Instagram, and other social sites are where people now voice their hostility, anger, or plans for malicious or violent activity.

And this phenomenon will only grow with time. Digital natives (those raised in the Internet age) are filling the ranks of organizations. Unlike their parents who typically use mainstream platforms Twitter and Facebook, younger employees tend to express themselves more expansively via a widening array of social media outlets. Whether posting about themselves or others, the information can provide valuable insights about a potential insider's perceptions, plans, and intentions.

Taken together, these forces have moved public data usage from a desirable—but optional—element of insider threat programs to becoming a critical resource. In today's world, failure to leverage such a resource leaves an organization, its employees, and its leadership open to financial, reputational, and physical risk. From an enterprise risk prevention perspective, public data cannot be ignored.

THE VALUE OF PUBLIC DATA SOURCES

Effective insider threat early warning rests on an organization's ability to understand its employees and their potential reactions to critical events so that problems can be identified and addressed before they result in harmful action. Used legally and properly, public data can help accomplish this.

Specifically, public data can be extremely valuable in assessing prospective hires, continuously evaluating trusted employees, and informing insider threat investigations by enabling the recognition of dangerous personality pre-dispositions, anomalous activity, and malicious behavior. With the move toward remote work, public data provides an opportunity to recognize atypical behavior that would otherwise go unnoticed or unreported.

Of the data publicly available to organizations, social media, financial data, and legal records are the ones most used for insider threat mitigation.

SOCIAL MEDIA

Whether it's a post about themselves or a post from others about them, social media now reflects what people are thinking and doing. As such, it can offer an open portal to an individual's state of mind and activities.

Facebook, Twitter, Instagram, LinkedIn, and other platforms may reflect unusually negative sentiment an insider feels toward an employer, colleagues, or others. It may also

reflect uncommon levels of risk-taking, such as an interest in criminal activity. On a broader scale, an individual's online affiliations can provide insights into his or her predisposition toward violence, fraud, or intellectual property theft. Finally, undisclosed foreign governmental or commercial affiliations may indicate espionage-related relationships and activity.

That said, the fluid nature of factors relevant to social media usage means that organizations need to proceed prudently before incorporating it into insider threat programs. These factors include how the public is using social media, the growing number and type of personal details being shared, the availability of stronger data analytics, and the evolution of privacy expectations and laws.

the fluid nature of factors relevant to social media usage means that organizations need to proceed prudently before incorporating it into insider threat programs.

A good example of how privacy concerns are evolving the law is the European Union's General Data Protection Regulation (GDPR). The regulation created privacy protections and generally requires organizations obtain explicit consent to collect, store, and process individual's data. It requires that employers only view an employee's social media profiles when the information is relevant to the position. Before doing so, employers need to undertake several actions, including notifying candidates before viewing their social media accounts and obtaining informed consent. Candidates and employees should also know exactly what their consent means, what information they are giving access to, and how that information will be used.

GDPR may be the bellwether for future U.S. privacy rulings because current U.S. law is more lenient.

U.S. employers monitoring U.S.-based employees are allowed to use publicly stated views to help determine if an individual may harm themselves, their colleagues, or the interests of the organization, and also as an element into broader analysis of an employee's ability to hold a position of trust.

FINANCIAL DATA

While personal financial situations have often proven themselves to be missed red flag indicators of insider data theft and fraud cases, it is not rare for saboteurs and those mounting violent workplace attacks to also be under financial stress. Simply put, financial issues have been recognized be early warning indicators in a variety of insider attack formats. Credit and tax reports can reveal delinquencies, foreclosures, recoveries, bankruptcies, and other problems that an employer should be aware of. With this early warning, employers can provide the assistance needed to prevent an insider from harming the organization.

LEGAL RECORDS

As noted, the path an insider takes from predisposition to action often provides indications of strife and turmoil within the insider's life. Law enforcement and court records can bring such turmoil in an employee's life to light.

Investigations, arrests, convictions, civil suits, and protective orders may indicate unpredictability, volatility, strained personal relations, addiction, or an inability to follow laws and established procedures.

Law enforcement involvement in an employee's life can also reflect drug, alcohol, sexual, and psychological problems. When viewed in the aggregate, independent events may indicate the employee should receive help or be removed from a position of trust.

STRATEGIC CONSIDERATIONS

As hinted above, incorporating public data into insider threat and continuous evaluation programs can be challenging. Firms must determine whether they feel the use of public data is merited and appropriate, and then come to a decision that fits their legal interpretations and corporate cultures. This decision making is individualistic, often based upon a cost–benefit analysis comparing the value of expected insider threat detection and deterrence versus the impact on employee morale and attrition.

To minimize potentially negative workforce perceptions, some organizations may decide to use public data that is somewhat invisible to employees—such as commercially available databases containing information on personal finances, credit, and law enforcement encounters—rather than more personal information like social media content.

The following questions may help leaders determine if their organizations should use public data as an element of their insider threat program:

- What data will reliably contribute to insider threat risk mitigation?
- Can the data be legally collected and assessed?
- Can the data be efficiently and effectively processed and analyzed?
- What internal policies must be implemented before using the data?
- What will be the impact on organizational culture and employee morale?
- Is the organization and its leadership comfortable using the data?

TACTICAL CONSIDERATIONS

If an organization decides to use public data for insider threat purposes, the following practices can help it do so effectively.

Ensure legal compliance, well-communicated governance and leadership support. All insider threat programs must comply with relevant privacy regulations, and organizations should employ proper legal expertise to understand and navigate them.

Within the United States, the Fair Credit Reporting Act (FCRA) and Equal Employment Opportunity Commission (EEOC) are the leading federal laws and regulators. Within the European Union, the GDPR is the leading regulation (see above).

All insider threat programs must comply with relevant privacy regulations, and organizations should employ proper legal expertise to understand and navigate them.

While compliance methods depend on jurisdiction, organizations must be prepared to provide the applicant or employee a written explanation of the use of public data for decisions about their employment, describe the nature and scope of the investigation, and obtain written permission.

Getting employee acceptance of the use of public data as an insider risk mitigation resource can be greatly enhanced by the way the organization plans, promotes, and implements its efforts. Clear policies and procedures must be crafted to ensure that the monitoring of data occurs only when warranted and is focused on assisting employees to avoid harmful situations.

Employees should be advised how public data can be used to identify situations that could financially or physically harm them, and how it will not be used. Consideration should be given to matching the use of public data to the position that an individual occupies; someone with greater access or responsibility receives greater scrutiny than

someone holding a more routine position. This governance should be incorporated into hiring documents so that prospective employees are fully aware of, and consent to, public data-based monitoring before they begin onboarding.

C-suite leadership should be open and consistent in its support for the proper use of public data for insider risk reduction; endorsing and promoting it as a valid security tool that can be used in a manner consistent with the organization's mission, culture, and values. Without such support, public data usage may cause resentment and pushback from the workforce.

To further promote trust, leadership should highlight the point that employees are able to redress information used to make personnel decisions. Specifically, the individual must have access to the raw data collected from publicly available (and other) sources to challenge, correct, or dispute it.

Leadership should highlight the point that employees are able to redress information used to make personnel decisions.

Use only relevant data. Employers need not respond to every foolish action an employee undertakes outside the workplace, but instead be focused on activities that indicate an employee poses a potential risk to him or herself, coworkers, facilities, or sensitive information. Program managers should develop criteria that identify the kinds of data that are relevant to workplace security, the data sources that meet these standards, and the types of potentially derogatory insights that merit further investigation.

Data should never be the sole determinant for decision making. Rather than considering derogatory information identified through public data as a demonstration that someone is untrustworthy, insider threat program

managers should treat indicators as a trigger for in-depth evaluation. In other words, public data should not be used in isolation to make personnel decisions; it must be placed in the context of an individual's broader life circumstances.

Remember that past behavior is not always an indicator of similar future behavior. Old expressions may not reflect a person's current beliefs or activities, and prior self-destructive habits (such as excessive drinking or gambling) may no longer be an issue. Indications of past financial difficulties may not accurately reflect one's current financial health. To summarize, information on past actions must be evaluated in the context of an employee's current personal and professional behavior.

Data usage must evolve with legal, technological, and cultural changes. The digital domain, social media, and online privacy issues are evolving. Advances in deep fake technologies, machine learning, 5G networks, quantum computing, and artificial intelligence are happening every day. While advances in data science may enable more efficient and effective use of public data for insider threat mitigation, other advances may prompt greater privacy controls.

As such, organizations must maintain a current understanding of new developments and their application to public data usage. If a new source of information meets established criteria for relevance and usefulness for insider threat analysis, an organization should consider whether and how to incorporate it into its evaluation protocol. The goal is to adopt technology that effectively identifies and ingests relevant data, ensures it conforms to organizational policies, compares or adds it to information gathered from internal sources, and packages it for evaluation by a skilled insider threat analyst.

The scope of opportunities for stopping insider attacks often goes underappreciated. Public data usage is one way to improve the identification of malicious insiders before they cause damage to an organization's information, people, or facilities.

VAL LETELLIER HAS 30 YEARS OF RISK MANAGEMENT EXPERIENCE IN THE PUBLIC AND PRIVATE SECTOR. HE RAN SECURITY OPERATIONS AS A U.S. STATE DEPARTMENT DIPLOMATIC SECURITY SPECIAL AGENT AND THEN INTELLIGENCE AND COUNTERINTELLIGENCE OPERATIONS AS A CIA OPERATIONS OFFICER AND STATION CHIEF. TWENTY YEARS SPENT RECRUITING FOREIGN SOURCES AND PENETRATING INTELLIGENCE TARGETS PROVIDED A DEEP UNDERSTANDING OF HOW INSIDERS ARE CREATED, MANAGED, PROTECTED, AND DISCOVERED. SUBSEQUENTLY, HE COFOUNDED A CYBERSECURITY FIRM THAT COMBINED CIA HUMAN SOURCE AND NSA TECHNICAL EXPERTISE. HE CONTINUES TO SUPPORT THE INTELLIGENCE COMMUNITY AND PROVIDES PRO-BONO INSIDER RISK ADVISEMENT TO WASHINGTON, D.C., CHARITIES AND NON-PROFITS. HE HOLDS AN MBA, MS, CISSP, CEH, ITVA, AND PMP. HE LEADS THE ASIS DEFENSE & INTELLIGENCE INSIDER THREAT WORKING GROUP AND IS A MEMBER OF THE INSA INSIDER THREAT SUBCOMMITTEE.

SECURITY MANAGEMENT

The Unique Threat of Insiders

Four years after the Snowden leaks, security professionals are still learning how to identify and prevent insider threats.

By Megan Gates

It's perhaps the most infamous incident of an insider threat in modern times. During the spring and summer of 2013, then-National Security Agency (NSA) contractor and Sharepoint administrator Edward Snowden downloaded thousands of documents about the NSA's telephone metadata mass surveillance program onto USB drives, booked a flight to Hong Kong, and leaked those documents to the media.

An international manhunt was launched, Snowden fled to Moscow, hearings were held in the U.S. Congress, and new policies were created to prevent another insider breach. The damage a trusted insider can do to an organization became painfully obvious.

"If you'd asked me in the spring of 2013...what's the state of your defense of the business proposition as it validates the technology, people, and procedures? I would have said, 'Good.

Not perfect,'" said Chris Inglis, former deputy director and senior civilian leader of the NSA during the Snowden leaks, in a presentation at the 2017 RSA Conference in San Francisco.

"I would have said that 'we believe, given our origins and foundations, and folks from information assurance, that that's a necessary accommodation," he explained. "We make it such that this architecture—people, procedure, and technology—is defensible."

Inglis also would have said that the NSA vetted insiders to ensure trustworthiness, gave them authority to conduct their jobs, and followed up with them if they exceeded that authority—intentionally or unintentionally—to remediate it.

"We made a critical mistake. We assumed that outsider external threats were different in kind than insider threats," Inglis said. "My view today is they are exactly the same. All of those are the exercise of privilege."

Inglis' perspective mirrors similar findings from the recent SANS survey *Defending Against the Wrong Enemy: 2017 Sans Insider Threat Survey* by Eric Cole, SANS faculty fellow and former CTO of McAfee and chief scientist at Lockheed Martin.

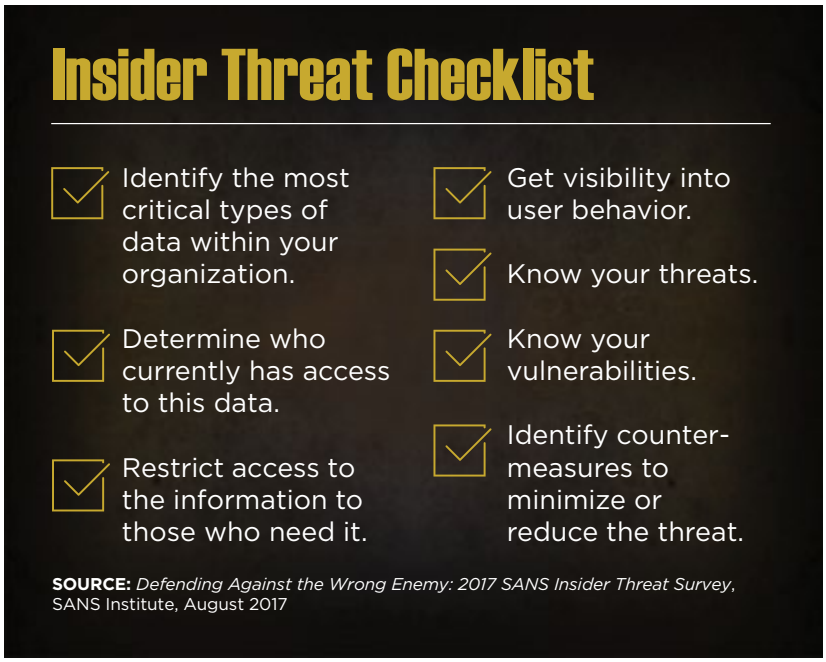
The SANS survey of organizations with 100 to 100,000 employees found that it can be easy to conclude that external attacks should be the main focus for organizations.

"This conclusion would be wrong. The critical element is not the source of a threat, but its potential for damage," Cole wrote. "Evaluating threats from that perspective, it becomes obvious that although most attacks might come from outside the organization, the most serious damage is done with help from the inside."

INSIDER THREAT PROGRAMS

Incidents like the Snowden leaks and the more recent case of Harold Thomas Martin III, an NSA contractor accused

of taking top secret information home with him, along with other incidents of economic espionage have raised awareness of the impact insider threats can have. However, many organizations have not adjusted their security posture to mitigate those threats.



In its survey, SANS found that organizations recognize insider threat as the "most potentially damaging component of their individual threat environments," according to the survey. "Interestingly, there is little indication that most organizations have realigned budgets and staff to coincide with that recognition."

Of the organizations surveyed, 49 percent said they are in the process of creating an insider threat program, but 31 percent still do not have a plan and are not addressing insider threats through such a plan.

"Unfortunately, organizations that lack effective insider threat programs are also unable to detect attacks in a timely manner, which makes the connection difficult to quantify," SANS found. "From experience, however, there is a direct

correlation between entities that ignore the problem and those that have major incidents."

Additionally, because many are not monitoring for insider threats, most organizations claim that they have never experienced an insider threat. "More than 60 percent of the respondents claim they have never experienced an insider threat attack," Cole wrote. "This result is very misleading. It is important to note that 38 percent of the respondents said they do not have effective ways to detect insider attacks, meaning the real problem may be that organizations are not properly detecting insider threats, not that they are not happening."

The survey also found that the losses from insider threats are relatively unknown because they are not monitored or detected. Due to this, organizations cannot put losses from insider threats into financial terms and may not devote resources to addressing the issue, making it difficult or impossible to determine the cost of an insider attack.

For instance, an insider could steal intellectual property and product plans and sell them to a competitor without being detected.

"Subsequent failure of that product might be attributed to market conditions or other factors, rather than someone 'stealing it,'" Cole wrote. "Many organizations, in my experience, are likely to blame external factors and only discover after detailed investigation that the true cause is linked back to an insider."

And when organizations do discover that an insider attack has occurred, most have no formal internal incident response plan to address it.

"Despite recognition of insiders as a common and vulnerable point of attack, fewer than 20 percent of respondents reported having a formal incident response plan that deals with insider threat," according to the SANS survey.

Instead, most incident response plans are focused on ex-

ternal threats, Cole wrote, which may explain why companies struggle to respond to insider threats.

Organizations are also struggling to deal with both malicious and accidental insider threats—a legitimate user whose credentials were stolen or who has been manipulated into giving an external attacker access to the organization. "Unintentional insider involvement can pose a greater risk, and considerably more damage, by allowing adversaries to sneak into a network undetected," the survey found. "Lack of visibility and monitoring capability are possible explanations for the emphasis on malicious insiders.

To begin to address these vulnerabilities, SANS recommends that organizations identify their most critical data, determine who has access to that data, and restrict access to only those who need it. Then, organizations should focus on increasing visibility into users' behavior to be proactive about insider threats.

We made a critical mistake. We assumed that outsider external threats were different in kind than insider threats.

"We were surprised to see 60 percent of respondents say they had not experienced an insider attack," said Cole in a press release. "While the confidence is great, the rest of our survey data illustrates organizations are still not quite effective at proactively detecting insider threats, and that increased focus on individuals' behaviors will result in better early detection and remediation."

TRUSTED PEOPLE

When the NSA recruits and hires people, it vets them thoroughly to ensure their trustworthiness, according to Inglis.

"We ultimately want to bring somebody into the enterprise who we can trust, give them some authority to operate within an envelope that doesn't monitor their tests item by item," he explained. "Why? Because it's within that envelope that they can exceed your expectations and the adversary's expectations, your competitors' expectations, and hopefully the customers' expectations. You want them to be agile, creative, and innovative."

To do this, the NSA would go to great lengths to find people with technical ability and possible trustworthiness. Then it or a third party would vet them, looking at their finances and their background, conducting interviews with people who knew them, and requiring polygraph examinations.

After the Snowden leaks, the U.S. federal government examined the work of its contract background screening firm—United States Investigations Services (USIS). USIS had cleared both Snowden and the Washington Navy Yard shooter Aaron Alexis. The government decided to reduce its contracted work with the company.

USIS later agreed to pay $30 million to settle U.S. federal fraud charges, forgoing payments that it was owed by the U.S. Office of Personnel Management for conducting background checks. The charges included carrying out a plot to "flush" or "dump" individual cases that it deemed to be low level to meet internal USIS goals, according to *The Hill's* coverage of the case.

"Shortcuts taken by any company that we have entrusted to conduct background investigations of future and current federal employees are unacceptable," said Benjamin Mizer, then head of the U.S. Department of Justice's Civil Division, in a statement. "The Justice Department will ensure that those who do business with the government provide all of the services for which we bargained."

This part of the process—vetting potential employees and

conducting background checks—is where many private companies go wrong, according to Sandra Stibbards, owner and president of Camelot Investigations and chair of the ASIS International Investigations Council.

"What I've come across many times is companies are not doing thorough backgrounds, even if they think they are doing a background check—they are not doing it properly," she says.

For instance, many companies will hire a background screening agency to do a check on a prospective employee. The agency, Stibbards says, will often say it's doing a national criminal search when really it's just running a name through a database that has access to U.S. state and county criminal and court records that are online.

"But the majority of counties and states don't have their criminal records accessible online," she adds. "To really be aware of the people that you're getting and the problem with the human element, you need to have somebody who specializes and you need to...invest the money in doing proper background checks."

To do this, a company should have prospective employees sign a waiver that informs them that it will be conducting a background check on them. This check, Stibbards says, should involve looking at criminal records in every county and state the individual has lived in, many of which will need to be visited in person.

She also recommends looking into any excessive federal court filings the prospective employee may have made.

"I'll look for civil litigation, especially in the federal court because you get people that are listed as a plaintiff and they are filing suits against companies for civil rights discrimination, or something like that, so they can burn the company and get money out of it," Stibbards adds.

Additionally, Stibbards suggests looking for judgments, tax liens, and bankruptcies, because that gives her perspective on whether a person is reliable and dependable.

"It's not necessarily a case breaker, but you want to have the full perspective of if this person is capable of managing themselves, because if they are not capable of managing themselves, they may not make the greatest employee," she says.

Companies should ensure that their background screenings also investigate the publicly available social media presence of potential employees. Companies can include information about this part of the process in the waiver that applicants sign agreeing to a background check to avoid legal complications later on.

"I'm going to be going online to see if I see chatter about them, or if they chat a lot, make comments on posts that maybe are inappropriate, if they maintain Facebook, LinkedIn, and Twitter," Stibbards says.

Posting frequently to social media might be a red flag. "If you find somebody on Facebook that's posting seven, eight, nine, or 10 times a day, this is a trigger point because social

media is more important to them than anything else they are doing," Stibbards adds.

And just because a prospective employee is hired doesn't mean that the company should discontinue monitoring his or her social media. While ongoing review is typically a routine measure, it can lead to disciplinary action for an employee who made it through the initial vetting process. For instance, Stibbards was hired by a firm to investigate an employee after the company had some misgivings about certain behaviors.

The critical element is not the source of a threat, but its potential for damage.

"Not only did we find criminal records that weren't reported, but we then found social media that indicated that the employee was basically a gang member—pictures of guns and the whole bit," Stibbards says.

It's also critical, once a new employee has been brought on board, to introduce him or her to the culture of the organization—an aspect that was missing in Snowden's onboarding process, Inglis said. This is because, as a contractor working for the NSA, regulations prohibited the U.S. government from training him.

"You show up as a commodity on whatever day you show up, and you're supposed to sit down, do your work—sit down, shut up, and color within the lines," Inglis explained.

So on Snowden's first day at the NSA, he was not taken to the NSA Museum like other employees and taught about the agency's history, the meaning of the oath new employees take, and the contributions the NSA makes to the United States.

"Hopefully there are no dry eyes at that moment in time, having had a history lesson laying out the sense of the vi-

tality and importance of this organization going forward," Inglis explained. "We don't do that with contractors. We just assume that they already got that lesson."

If companies fail to introduce contractors and other employees to the mission of the organization and its culture, those employees will not feel that they are part of the organization.

TRUSTED TECHNOLOGY

Once trusted people are onboarded, companies need to evaluate their data—who has access to it, what controls are placed on it to prevent unwarranted access, and how that access is monitored across the network.

"The one thing I always recommend to any company is to have a monitoring system for all of their networks; that is one of the biggest ways to avoid having issues," Stibbards says. "Whether it's five people working for you or 100, if you let everybody know and they are aware when they are hired that all systems—whether they are laptops or whatever on the network—are all monitored by the company, then you have a much better chance of them not doing anything inappropriate or...taking information."

These systems can be set up to flag when certain data is accessed or if an unusual file type is emailed out of the network to another address.

Simon Gibson, fellow security architect at Gigamon and former CISO at Bloomberg LP, had a system like this set up at Bloomberg, which alerted security staff to an email sent out with an Adobe PDF of an executive's signature.

"He's a guy who could write a check for a few billion dollars," Gibson explains. "His signature was detected in an email being sent in an Adobe PDF, and it was just his signature...of course the only reason you would do that is to forge it, right?"

So, the security team alerted the business unit to the potential fraud. But after a quick discussion, the team found

that the executive's signature was being sent by a contractor to create welcome letters for new employees.

"From an insider perspective, we didn't know if this was good or bad," Gibson says. "We just knew that this guy's signature probably ought not be flying in an email unless there's a really good reason for it."

Thankfully, Bloomberg had a system designed to detect when that kind of activity was taking place in its network and was able to quickly determine whether it was malicious. Not all companies are in the same position, says Brian Vecci, technical evangelist at Varonis, an enterprise data security provider.

In his role as a security advocate, Vecci goes out to companies and conducts risk assessments to look at what kinds of sensitive data they have. Forty-seven percent of companies he's looked at have had more than 1,000 sensitive data files that were open to everyone on their network. "I think 22 percent had more than 10,000 or 12,000 files that were open to everybody," Vecci explains. "The controls are just broken because there's so much data and it's so complex."

To begin to address the problem, companies need to identify what their most sensitive data is and do a risk assessment to understand what level of risk the organization is exposed to. "You can't put a plan into place for reducing risk unless you know what you've got, where it is, and start to put some metrics or get your arms around what is the risk associated to this data," Vecci says.

Then, companies need to evaluate who should have access to what kinds of data, and create controls to enforce that level of access.

This is one area that allowed Snowden to gain access to the thousands of documents that he was then able to leak. Snowden was a Sharepoint administrator who populated a server so thousands of analysts could use that information to chase threats. His job was to understand how the NSA col-

lects, processes, stores, queries, and produces information.

"That's a pretty rich, dangerous set of information, which we now know," Inglis said. "And the controls were relatively low on that—not missing—but low because we wanted that crowd to run at that speed, to exceed their expectations."

Following the leaks, the NSA realized that it needed to place more controls on data access because, while a major leak like Snowden's had a low probability of happening, when it did happen the consequences were extremely high.

"Is performance less sufficient than it was before these maneuvers? Absolutely," Inglis explained. "But is it a necessary alignment of those two great goods—trust and capability? Absolutely."

Following the leaks, the NSA realized that it needed to place more controls on data access because, while a major leak like Snowden's had a low probability of happening, when it did happen the consequences were extremely high.

Additionally, companies should have a system in place to monitor employees' physical access at work to detect anomalies in behavior. For instance, if a system administrator who normally comes to work at 8:00 a.m. and leaves at 5:00 p.m. every day, suddenly comes into the office at 2:00 a.m. or shows up at a workplace with a data storage unit that's not in his normal rotation, his activity should be a red flag.

"That ought to be a clue, but if you're not connecting the dots, you're going to miss that," Inglis said.

TRUSTED PROCESSES

To truly enable the technology in place to monitor network traffic, however, companies need to have processes to respond to anomalies. This is especially critical because

often the security team is not completely aware of what business units in the company are doing, Gibson says.

While at Bloomberg, his team would occasionally get alerts that someone had sent software—such as a document marked confidential—to a private email address. "When the alert would fire, it would hit the security team's office and my team would be the first people to open it and look at it and try analyze it," Gibson explains. "The problem is, the security team has no way of knowing what's proprietary and valuable, and what isn't."

To gather this information, the security team needs to have a healthy relationship with the rest of the organization, so it can reach out to others in the company—when necessary—to quickly determine if an alert is a true threat or legitimate business, like the signature email.

Companies also need to have a process in place to determine when an employee uses his or her credentials to inappropriately access data on the network, or whether those credentials were compromised and used by a malicious actor.

Gibson says this is one of the main threats he examines at Gigamon from an insider threat perspective because most attacks are carried out using people's credentials. "For the most part, on the network, everything looks like an insider threat," he adds. "Take our IT administrator—someone used his username and password to login to a domain controller and steal some data...I'm not looking at the action taken on the network, which may or may not be a bad thing, I'm actually looking to decide, are these credentials being used properly?"

The security team also needs to work with the human resources department to be aware of potential problem employees who might have exceptional access to corporate data, such as a system administrator like Snowden.

For instance, Inglis said that Snowden was involved in a workplace incident that might have changed the way he felt about his work at the NSA. As a systems administrator with incredible access to the NSA's systems, Inglis said it would have made sense to put a closer watch on him after that incident in 2012, because the consequences if Snowden attacked the NSA's network were high.

"You cannot treat HR, information technology, and physical systems as three discrete domains that are not somehow connected," Inglis said.

Taking all of these actions to ensure that companies are hiring trusted people, using network monitoring technology, and using procedures to respond to alerts, can help prevent insider threats. But, as Inglis knows, there is no guarantee.

"Hindsight is 20/20. You have to look and say, 'Would I theoretically catch the nuances from this?'" ◪

CONTACT ASSOCIATE EDITOR MEGAN GATES AT *MEGAN.GATES@ASISONLINE.ORG.* OR ON TWITTER *@MGNGATES.*

SECURITY
MANAGEMENT

How to Hack a Human

When cybersecurity measures become difficult to penetrate by technical means, people become the weakest link in the system.

By Scott Stewart

It all started innocuously with a Facebook friend request from an attractive woman named Mia Ash. Once her request was accepted, she struck up a conversation about various topics and showed interest in her new friend's work as a cybersecurity expert at one of the world's largest accounting firms.

Then, one day Mia shared her dream—to start her own company. She had one problem, though; she did not have a website and did not know how to create one. Surely her new friend could use his expertise to help her achieve her dreams by helping her make one?

Mia said she could send him some text to include on the new site. He agreed, and when he received a file from Mia he opened it—on his work computer. That simple act launched a malware attack against his company resulting in a significant compromise of sensitive data.

Mia was not a real person, but a care-fully crafted online persona created by a prolific group of Iranian hackers—known as Oilrig—to help this elaborate spear phishing operation succeed.

Due to his role in cybersecurity, the target was unlikely to have fallen for a standard phishing attack, or even a normal spear phishing operation. He was too well trained for that. But nobody had prepared him for a virtual honey trap, and he fell for the scheme without hesitation.

This case is a vivid reminder that when cybersecurity measures become difficult to penetrate by technical means, people become the weakest link in a cybersecurity system. It also illustrates how other intelligence tools can be employed to help facilitate cyber espionage.

While many hackers are merely looking to exploit whatever they can for monetary gain, those engaging in cyber espionage are different. They are often either working directly for a state or large nonstate actor, or as a mercenary contracted by such an actor tasked with obtaining specific information.

This targeted information typically pertains to traditional espionage objectives, such as weapons systems specifications or the personal information of government employees—like that uncovered in the U.S. Office of Personnel Management hack.

The information can also be used to further nondefense-related economic objectives, such as China's research and design 863 program, which was created to boost innovation in high-tech sectors in China.

Given this distinction and context, it is important to understand that hacking operations are just one of the intelligence tools sophisticated cyber espionage actors possess. Hacking can frequently work in conjunction with other intelligence tools to make them more efficient.

Hacking into the social media accounts or cell phone of a person targeted for a human intelligence recruitment operation can provide a goldmine of information that can greatly assist those determining the best way to approach the target.

For instance, hacking into a defense contractor's email account could provide important information about the date, time, and place for the testing of a revolutionary new technology. This information could help an intelligence agency focus its satellite imagery, electronic surveillance, and other collection systems on the test site.

Nobody had prepared him for a virtual honey trap, and he fell for the scheme without hesitation.

Conversely, intelligence tools can also be used to enable hacking operations. Simply put, if a sophisticated cyber espionage actor wants access to the information contained on a computer system badly enough, and cannot get in using traditional hacking methods, he or she will use other tools to get access to the targeted system. A recent case in Massachusetts illustrates this principle.

Medrobotics CEO Samuel Straface was leaving his office at about 7:30 p.m. one evening when he noticed a man sitting in a conference room in the medical technology company's secure area, working on what appeared to be three laptop computers.

Straface did not recognize the man as an employee or contractor, so he asked him what he was doing. The man replied that he had come to the conference room for a meeting with the company's European sales director. Straface informed him that the sales director had been out of the country for three weeks.

The man then said he was supposed to be meeting with Medrobotics' head of intellectual property. But Straface told him the department head did not have a meeting scheduled for that time.

Finally, the man claimed that he was there to meet the CEO. Straface then identified himself and more strongly confronted the intruder, who said he was Dong Liu—a lawyer doing patent work for a Chinese law firm. Liu showed Straface a LinkedIn profile that listed him as a senior partner and patent attorney with the law firm of Boss & Young.

Straface then called the police, who arrested Liu for trespassing and referred the case to the FBI. The Bureau then filed a criminal complaint in the U.S. District Court for the District of Massachusetts, charging Liu with one count of attempted theft of trade secrets and one count of attempted access to a computer without authorization. After his initial court appearance, Liu was ordered held pending trial.

Straface caught Liu while he was presumably attempting to hack into the company's Wi-Fi network. The password to the firm's guest network was posted on the wall in the conference room, and it is unclear how well it was isolated from the company's secure network. It was also unknown whether malware planted on the guest network could have affected the rest of the company's information technology infrastructure.

The fact that the Chinese dispatched Liu from Canada to Massachusetts to conduct a black bag job—an age-old intelligence tactic to covertly gain access to a facility—indicates that it had not been able to obtain the information it desired remotely.

China had clear interest in Medrobotics' proprietary information. Straface told FBI agents that companies from China had been attempting to develop a relationship with the company for about 10 years, according to the FBI affidavit.

Straface said he had met with Chinese individuals on about six occasions, but ultimately had no interest in pursuing business with the Chinese.

Straface also noted that he had always met these individuals in Boston, and had never invited them to his company's headquarters in Raynham, Massachusetts. This decision shows that Straface was aware of Chinese interest in his company's intellectual property and the intent to purloin it. It also shows that he consciously attempted to limit the risk by keeping the individuals away from his facilities. Yet, despite this, they still managed to come to the headquarters.

Black bag attacks are not the only traditional espionage tool that can be employed to help facilitate a cyberattack. Human intelligence approaches can also be used.

In traditional espionage operations, hostile intelligence agencies have always targeted code clerks and others with access to communications systems.

Other intelligence tools can be employed to help facilitate cyber espionage.

Computer hackers have also targeted humans. Since the dawn of their craft, social engineering—a form of human intelligence—has been widely employed by hackers, such as the Mia Ash virtual honey trap that was part of an elaborate and extended social engineering operation.

But not all honey traps are virtual. If a sophisticated actor wants access to a system badly enough, he can easily employ a physical honey trap—a very effective way to target members of an IT department to get information from a company's computer system. This is because many of the lowest paid employees at companies—the entry level IT

staff—are given access to the company's most valuable information with few internal controls in place to ensure they don't misuse their privileges.

Using the human intelligence approaches of MICE (money, ideology, compromise, or ego), it would be easy to recruit a member of most IT departments to serve as a spy inside the corporation. Such an agent could be a one-time mass downloader, like Chelsea Manning or Edward Snowden.

Or the agent could stay in place to serve as an advanced, persistent, internal threat. Most case officers prefer to have an agent who stays in place and provides information during a prolonged period of time, rather than a one-time event.

IT department personnel are not the only ones susceptible to such recruitment. There are a variety of ways a witting insider could help inject malware into a corporate system, while maintaining plausible deniability. Virtually any employee could be paid to provide his or her user ID and password, or to intentionally click on a phishing link or open a document that will launch malware into the corporate system.

An insider could also serve as a spotter agent within the company, pointing out potential targets for recruitment by directing his or her handler to employees with marital or financial issues, or an employee who is angry about being passed over for a promotion or choice assignment.

An inside source could also be valuable in helping design tailored phishing attacks. For instance, knowing that Bob sends Janet a spreadsheet with production data every day, and using past examples of those emails to know how Bob addresses her, would help a hacker fabricate a convincing phishing email.

Insider threats are not limited only to the recruitment of current employees. There have been many examples of the

Chinese and Russians recruiting young college students and directing them to apply for jobs at companies or research institutions in which they have an interest.

In 2014, for instance, the FBI released a 28-minute video about Glenn Duffie Shriver—an American student in Shanghai who was paid by Chinese intelligence officers and convicted of trying to acquire U.S. defense secrets. The video was designed to warn U.S. students studying abroad about efforts to recruit them for espionage efforts.

Chief information security officers need to work hand-in-glove with chief security officers, human resources, legal counsel, and others if they hope to protect the companies and departments in their charge.

Because of the common emphasis on the cyber aspect of cyber espionage—and the almost total disregard for the role of other espionage tools in facilitating cyberattacks—cyber espionage is often considered to be an information security problem that only technical personnel can address.

But in the true sense of the term, cyber espionage is a much broader threat that can emanate from many different sources. Therefore, the problem must be addressed in a holistic manner.

Chief information security officers need to work hand-in-glove with chief security officers, human resources, legal counsel, and others if they hope to protect the companies and departments in their charge.

When confronted by the threat of sophisticated cyber espionage actors who have a wide variety of tools at their disposal, employees must become a crucial part of their employers' defenses as well.

Many companies provide cybersecurity training that includes warnings about hacking methods, like phishing and social engineering, but very few provide training on how to spot traditional espionage threats and tactics. This frequently leaves most workers ill prepared to guard themselves against such methods.

Ultimately, thwarting a sophisticated enemy equipped with a wide array of espionage tools will be possible only with a better informed and more coordinated effort on the part of the entire company.

SCOTT STEWART IS VICE PRESIDENT OF TACTICAL ANALYSIS AT STRATFOR.COM AND LEAD ANALYST FOR STRATFOR THREAT LENS, A PRODUCT THAT HELPS CORPORATE SECURITY PROFESSIONALS IDENTIFY, MEASURE, AND MITIGATE RISKS THAT EMERGING THREATS POSE TO THEIR PEOPLE, ASSETS, AND INTERESTS AROUND THE GLOBE.

SECURITY MANAGEMENT

Paved With Good Intentions

With unrealistic goals and high pressure, incentives to perform can become incentives to cheat. Mindful managers can reduce the likelihood of unintended consequences.

By Mark Tarallo

The incentive may have seemed ordinary when Wells Fargo management first issued it. But it led to some extraordinarily negative consequences.

Wells managers imposed what was sometimes called an "Eight is Great" target for their employees: sell eight accounts per customer. This type of cross-selling, in which bank employees encourage account holders to open another account, take out a credit card, or buy other services, is a common method for companies in the banking industry to increase their revenue.

But in late 2016, according to news reports and testimony before the U.S. Congress, company representatives publicly conceded that the incentive resulted in disaster. Over a period of at least five years, Wells Fargo employees created more than 1.5 million unauthorized deposit accounts, and at least 500,000 unauthorized credit card applications.

POLLUTED ECOSYSTEM

The Wells Fargo case was a clear example of a perverse incentive—an incentive that results in unintended and undesirable consequences contrary to the interests of the incentive designers.

For managers, it's important to recognize that all incentives have the potential to turn perverse, says managerial incentive expert Marc Hodak of Farient Advisors.

"Every incentive to perform is an incentive to cheat. You can't have one without the other," he says.

In practice, the majority of incentives or performance targets in the business world do not turn perverse, despite the potential to do so. Why so with Wells Fargo?

Hodak says that a few factors came together in the Wells case, and collectively they sustained a "perverse incentive ecosystem."

"Any one of the factors individually wouldn't have resulted in the debacle [that happened]," Hodak explains.

One crucial factor, Hodak says, was an unrealistic goal. While cross selling is common in the industry, eight accounts per customer, even as an aspirational goal, does not seem realistically achievable on a widespread scale.

Other factors compounded this problematic goal, Hodak explains. High-level managers were offered lucrative financial rewards if their staff hit the targets, and managers' bonuses were dependent on the degree to which sales goals were achieved. By some accounts, certain Wells managers began checking their progress toward the sales goals twice a day, thus helping to create an office environment that felt like a pressure cooker.

In addition to rewards for upper management, incentives were also offered at lower levels of the organization, such as promotions and job security for sales staff who fulfilled the performance goals.

Still, in most other companies, these factors do not blow up into a catastrophic situation, because there is usually some sort of safety valve. For example, some companies have an internal system of controls that flags suspicious activity, such as an unusual surge in new account creation.

But at Wells Fargo, the situation was not checked internally and it spiraled out of control. Managers communicated to employees that there would be penalties for not reaching the goals, thereby increasing the possibility of risky behavior. And management punished some who complained.

"The safety valve got short circuited somehow," Hodak says. "The cheats were getting ahead, and the honest were afraid of getting fired."

A VARIETY OF PERVERSITIES

Of course, the Wells Fargo sales goals are not the only type of perverse incentive. While they can take different forms, management experts say that there are a few specific types of incentive that can run into problems.

One is an undermining metric. This type of metric may fulfill a short-term goal, but it is ultimately not in the organization's long-term interest.

Every incentive to perform is an incentive to cheat. You can't have one without the other.

For example, a company that wants to become more prepared for an active shooter incident may decide to require an annual active shooter training session. Once the session is complete, company leaders then say they have fulfilled their goal.

But it is possible that the training was ineffective, so the metric has the unintended or perverse effect of convincing

managers that the company is prepared, even though it is not. Instead of this metric, the company should focus on performance improvement metrics that can measure the effectiveness of the training.

Another type of perverse incentive, experts say, can come in the form of budget pressure. Company leaders may indicate to the security manager that proposed budget reductions will be looked favorably upon, because they will save the company money. The security manager may then make personnel cuts that can be covered for in the short term, which are approved by the CEO. But in the long term, they may have the unintended effect of compromising the company's security.

Company leaders may indicate to the security manager that proposed budget reductions will be looked favorably upon, because they will save the company money.

Some financial rewards can also become perverse incentives if they alter an employee's motivation. When performance is rewarded with financial compensation, an employee's motivation can change, so that the driving force of his or her behavior becomes the extrinsic motivator of financial reward, not an intrinsic motivation to do good work.

This can have the unintended effect of decreasing an employee's overall intrinsic motivation, which can hurt performance in other areas. And studies show that reliance on extrinsic motivators can diminish creativity, which is an important component of learning and performance.

In addition, Hodak says that a performance target is more likely to have perverse effects if it contains an all-or-nothing threshold—that is, employees get a significant reward if they hit a goal of eight accounts per customer, but get nothing if they come close, like selling seven accounts.

AVOIDANCE STRATEGIES

In as much as no one can predict the future, no manager can guarantee that his or her company's incentives will never turn perverse. However, there are strategies for minimizing their likelihood, and in a recent interview with *Security Management*, veteran security manager Bill Wipprecht offered some best practice guidance.

Wipprecht was CSO for Wells Fargo for 23 years, until 2010. He was not involved in the incentive situation and was long gone when it came to light; he says he remembers Wells Fargo as a great company and great place to work, albeit with the business ups-and-downs that every firm experiences for creating incentives.

"I never saw the Wells Fargo incentive as being illegal. It was unethical," he says.

Wipprecht agrees with the argument that setting an unrealistic goal was one of the key reasons why the Wells incentive turned perverse. And that can sometimes be difficult to avoid, he adds, because most managers have done this at least occasionally in their career.

He gave the common example of a manager who sits with an underachieving employee in a review and sets an even higher performance goal, even though it seems unrealistic given past performance.

"Almost every manager has set unrealistic goals and objectives, and asked that the employee meet them," he says.

However, the pressure cooker atmosphere that can drive an incentive toward perversity can be avoided if managers self-regulate their own behavior, Wipprecht says. To illustrate, he gave the example of how a security manager deals with vendors.

"I've had managers call a vendor and beat them to a pulp for minor performance issues," he says. "It's almost abusive, and then what are you going to expect in return?"

What they might get, he adds, is a vendor who will say anything to avoid that type of abuse in the future, including unrealistic claims about the products or services being used that could lead to unintended negative consequences down the line.

Attitude checks by security managers are also useful in dealing with employees, he adds. Wipprecht remembers how, as CSO, his temperament set the tone of the department. When he was happy and smiling, his employees were too; on days when he came into the office in a bad mood, the department darkened.

"That was the mood for the entire office for the whole day," he says.

When the manager's darker moods strike, employees are more likely to present issues in a positive light. For example, they may pretend that their performance is higher than it really is, or they may avoid the manager altogether—even though a pressing security issue needs to be discussed.

I never saw the Wells Fargo incentive as being illegal. It was unethical.

Finally, friendly competition among employees may work to increase productivity, but managers need to realize that it's unwise "to set up an overly competitive situation in an organization, rather than a teamwork environment, which is what you want to instill," Wipprecht cautions.

Along the same lines, perceived favoritism can lead to unintended consequences, because employees may get the sense that the game is rigged, and they need to do something drastic to compete. "If you've got a favorite in the office, it sets a negative tone for the rest of employees," he says.

In the end, experts say that incentives can still be used in a positive fashion, but managers need to be continually mindful of where they could go wrong.

"Whenever you put [incentives] in play, you are playing with fire," Hodak says. "Fire is terribly useful, but it can also be dangerous."

CONTACT SENIOR EDITOR MARK TARALLO AT MARK.TARALLO@ASISONLINE.ORG. CONNECT WITH HIM ON LINKEDIN.

SECURITY MANAGEMENT

Personnel Peril

Well-rounded, consistent, insider threat programs can be built by private sector organizations by implementing low- or no-cost best practices.

By Ronald R. Newsom, CPP

When employees steal proprietary information, they don't just cause headaches for the organization—they erode confidence in the trustworthiness of screened employees and vetted business partners. Following the recent spate of high-profile incidents—including leaks by U.S. National Security Agency contractor Edward Snowden in 2013, violent attacks on Fort Hood by Major Nidal Hasan in 2009, and Washington Navy Yard shooter Aaron Alexis in 2013—the U.S. government determined that existing vetting processes and security standards for sensitive programs were inadequate. Key policy changes were implemented, including a new requirement for government organizations and certain government contractors to establish an insider threat program. The requirements changed the way government-affiliated organizations approached employee management and codified existing insider threat practices.

What does that mean for private sector organizations, even if they don't work with the government? Certain features of a U.S. Department of Defense (DoD)-style insider threat program may be relatively easy to implement and offer considerable security enhancements. Traditional administrative and physical

security practices—locked doors, alarm systems, and inventory controls—are focused externally and are largely ineffective at preventing employees and other authorized persons from committing harmful acts.

Integrating an insider threat policy with employee and event best practices can create a well-rounded employee management program that benefits workers and the organization. Educating employees on how to recognize and report potential insider threat information can also have a positive effect on the organization's culture and emphasize everyone's role in keeping a safe, secure work environment.

Concurrent Technologies Corporation (CTC), an independent, nonprofit organization that conducts applied scientific research and development for government and industry, faced this exact challenge upon the creation of a nuclear research facility.

With industrial space and laboratories in five states, and more than 25 percent of employees telecommuting, CTC's potential insider threat profile is typical among many technology companies in the United States. Protection of sensitive government programs, client information, and intellectual property is paramount to success in a highly competitive environment.

But the August 2017 establishment of CTC's Center for Advanced Nuclear Manufacturing (CANM) in Johnstown, Pennsylvania, created new insider threat challenges that CTC had to address. The CANM is designed to bring fabri-

cation technology and materials expertise to the emerging next generation of commercial nuclear power plants and will conduct business only with private sector organizations that are working on small nuclear reactors. While CTC works with both industry and sensitive government programs—and must abide by federal insider threat policies—it wanted CANM to have a government-grade insider threat program that would defend against all kinds of manmade threats—from petty theft to intellectual property issues to event management.

A planned ribbon cutting and open house event at the CANM would place about 75 visitors in close proximity to CTC's intellectual property and advanced technology—and would serve as the first real test of the organization's new insider threat policy.

TAILORING A SOLUTION

The FBI, U.S. Department of Homeland Security (DHS), and U.S. Defense Security Service provide tools for industry organizations to develop insider threat programs, including online training courses and brochures available through public websites. The tools identify specific behaviors that may indicate the presence of an insider threat.

Simply educating employees on what to watch for may improve the chances of averting a workplace incident. Other insider threat program features, such as information sharing and incident reporting, could also prove beneficial. Initiatives can be tailored to fit the organization, and security practitioners may find that their programs already include parts of the overall insider threat framework outlined in government directives.

This was true for CTC as it began to build a more robust insider threat program. While the organization had taken an informal approach to communicating potential employee

issues, it was nowhere near the formalized program needed. To make sure the program covered all threats, CTC created an insider threat working group.

Comprehensive support. An insider threat program relies on buy-in throughout the organization. A single official with authority to develop policies and procedures should be appointed to manage the program. He or she should also be responsible for determining when to report substantive insider threat information to law enforcement and other entities outside the organization.

An insider threat program relies on buy-in throughout the organization.

CTC appointed an insider threat program official and established a working group with membership based on relevant roles, including representatives from security, human resources, IT, executive management, and ethics and compliance. The working group conducted several program reviews and established the types of activities to watch out for or report.

The group also ensured that all employees completed awareness training in the time leading up to the CANM open house and helped foster a culture of communication so that employees would not hesitate to report concerns about visitors or fellow employees. Line employees are often the first to sense that something is off—if they notice changes in an employee's routine or behavior, they should know how to safely and effectively communicate the information to team leaders without fear of retribution.

Security staff and senior managers stood ready to work with department managers and labor representatives to reduce or eliminate social barriers to reporting. Reporting

policy violations and unusual or suspicious behavior must not be viewed as tattling. Instead, it should be emphasized that timely reporting may save the company or business unit from significant financial loss, unfair competition, or even a tragic incident.

Team approach. Effective information sharing and collaboration among security stakeholders in the organization are essential for a stalwart insider threat program. Functional leaders—like the ones in CTC's insider threat working group—typically monitor organizational performance in areas relevant to detecting a potential insider threat. For example, larger organizations usually rely on a CISO to detect violation or circumvention of policies regarding systems access, file transfers, software installation, and other network activities. Likewise, the human resources department should track, analyze, and share information on trends in employee misconduct, including harassment complaints and drug testing. In reviewing such information, the team must take care to protect employee privacy and focus only on security-relevant factors that might create concerns of an insider threat and identify needed adjustments in policies and training.

For special events and unusual situations, organizations should not shy away from reaching out for help. The CTC insider threat program's leader contacted the FBI private sector coordinator, Defense Security Service representatives, and local law enforcement officials several weeks before the open house to inform them about the event and to obtain updated threat information. The FBI coordinator participated in an event rehearsal and walkthrough, and provided a tailored counterintelligence briefing to CANM engineers, program managers, and support staff, offering specific recommendations to limit risk while accomplishing overall open house objectives.

Training. Employees should feel that they share a common security interest—success for themselves and for the entire organization requires their commitment to protecting intellectual property, proprietary information, and other valuable resources. Leaders must emphasize these points and encourage employees to actively support security programs and procedures. Employee commitment and loyalty to a common cause cannot be assumed, particularly in industries that experience high employee turnover.

Employees should feel that they share a common security interest—success for themselves and for the entire organization requires their commitment to protecting intellectual property, proprietary information, and other valuable resources.

Training employees to watch for specific activities and behaviors that may indicate an insider threat is the key to viable information reporting within the organization. Employees tend to recognize differences in a coworker's attitude, work ethic, or behavior well before an incident occurs, so they must know when and how to report concerns. Employees must also know how to recognize suspicious emails, scams, phishing attempts, and social engineering tricks to avoid becoming an unwitting insider or being coerced into providing information or other assistance. Training should also emphasize the importance of following basic rules aimed at mitigating risk, such as locking or switching off computer workstations when unattended.

CANM employees were trained in traditional insider threat identification messages but were also given tips on identifying and reporting suspicious behavior at the open house event.

Because engineers, program managers, and event staff integrated security best practices into their job requirements, enhanced security was everywhere yet remained unseen at the event.

Written plans. The insider threat working group at CTC identified all written guidance regarding employee behavior, from harassment policies and timekeeping systems to travel plans and procedures and integrated it into the plan. The insider threat program features a risk mitigation plan that identifies insider threat stakeholders, roles and responsibilities, resources, policies, and procedures. The team of stakeholders meet periodically to review the plan, share and assess potential insider threat information, and determine additional actions needed to protect people, operations, intellectual property, and other resources.

For example, at a stakeholder meeting, someone in charge of travel finances might point out that the rental car budget for the previous month was 20 percent larger than normal. Human resources personnel can revisit employee travel dates and potentially identify excessive use of rental vehicles for personal travel. The same insider threat reporting procedures should be followed to address the problem.

REDEFINING INSIDER THREATS

CTC's reevaluation and preparation paid off—the open house event went smoothly for staff and visitors alike. CTC security officials are also reaping longer-term benefits from the CANM experience. For example, the department is improving its approach to training by conducting lunchtime seminars and more personal interviews with employees to reinforce the significant role that each employee plays in countering insider threats, even if security is not their primary role.

In addition to the CANM program, other business changes prompted CTC to reassess potential threats and strengthen routine security procedures. New contracts with government clients outside the DoD brought new requirements and concerns for protecting sensitive information processed and stored on company networks. The company invested in new equipment, and other areas of business development brought increased interaction with international customers—along with added challenges for ensuring compliance with American export laws.

By thinking outside the box in regard to an insider threat, CDC was able to create a well-rounded employee management policy that is capable of addressing a variety of organizational concerns. Addressing a wide scope of potentially problematic employee-related activity—not just intellectual property or workplace violence concerns—through an insider threat lens strengthens the entire program and makes it more adaptable for addressing other business concerns.

As an example, security staff worked with shop floor staff and project managers to revise the facility's access control plan. Doors to certain industrial areas within the 250,000-square foot CANM were closed to employees who did not have a clear need for access. Facility access hours were restricted for many employees, and a proximity card in addition to a six-digit PIN is now required to use doors that are not routinely monitored. Process owners and senior managers fully grasped the need for such procedural changes and strongly supported the recommendations.

As international business contacts expanded, the security, contracts, and export compliance departments worked closely with program managers to ensure that export licenses encompass all international dealings involving protected technologies. The company's enterprise visitor

system, internally developed in 2012 and upgraded in 2015, electronically routes international visit requests for coordination and approval. This ensures that the right managers and technicians are informed, projects are shrouded, or operations are suspended or rescheduled as needed.

With such low- or no-cost security enhancements in place, establishing an insider threat program required only a modest effort to formalize plans and procedures, chartering a working group, and expanding existing training. Other corporations working exclusively or extensively with government contracts can engineer similar results.

Increasing awareness of insider threats and encouraging employees to report suspicious behavior and policy violations has directly led to improved overall security.

Increasing awareness of insider threats and encouraging employees to report suspicious behavior and policy violations has directly led to improved overall security. For example, information received in recent months from frontline employees has enabled managers to correct internal issues and mitigate vulnerabilities in how the company purchases, inventories, and accounts for low-cost supplies, equipment, and bench tools. Workers in the affected areas recognize how the changes reduce risk of pilferage and unauthorized use of company assets. Minimizing such losses helps the company control overhead costs, remain competitive, and protect jobs and salaries.

If an organization is unaccustomed to a regimen of safety and security rules during daily business operations, it may take months to evolve a security culture where employees

are likely to bring their concerns forward and key supervisors can evaluate information and respond effectively. The advantages of starting now almost certainly outweigh the risk of what could come later.

RONALD R. NEWSOM, CPP, IS A RETIRED U.S. AIR FORCE OFFICER NOW EMPLOYED WITH CONCURRENT TECHNOLOGIES CORPORATION, A RECIPIENT OF THE DOD 2017 COLONEL JAMES S. COGSWELL AWARD FOR SUSTAINED EXCELLENCE IN INDUSTRIAL SECURITY. NEWSOM IS A MEMBER OF ASIS INTERNATIONAL. HE ALSO SERVES AS THE CHAIR OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY'S APPALACHIAN CHAPTER.