Solving the enigmatic insider threat within

Insider threats can be malicious or accidental, but they are always a threat. Evan Schuman explores how to solve the puzzle with analytics.

At the risk of potentially alienating a high-demand workforce that potentially can jump to a new company for seemingly minor perks such as company-paid cafeterias or flex time with little oversight, CISOs today find themselves with a challenge. In order to protect their corporations against data breach from internal and external sources, CISOs have a tool that is effective at identifying breaches but some employees might find a bit too intrusive: analytics. The move to analytics-based security — be it behavioral, threat intelligence, big data, or one of a myriad of other analytics technologies — could be interpreted as Big Brother watching over the employees.

OUR EXPERTS: Cloud IAM

Doug Barbin, principal and cybersecurity practice leader, Schellman & Co.

Joseph Blankenship, principal analyst, Forrester

Anton Chuvakin, research vice president, distinguished analyst, Gartner

Catherine Flick, member, Association for Computing Machinery's Committee on Professional Ethics; reader, De Montfort University (United Kingdom)

David Pearson, principal threat researcher, Awake Security

Sean Pike, security products program vice president, IDC

Danny Rogers, CEO, Terbium Labs

The potential damage that an insider attack can inflict on a business is massive, a reality that prompted some enterprises to use analytics, keystroke capture, and digital video to track insiders. But are the risks of a company alienating its employees and contractors worth it? Are analytics even an effective means of neutralizing insider threats?

When exploring insider threats, it is critical to focus on the distinctions between a potential and an actual threat. The potential threat is significant with insider attacks, given that these are people who already have legitimate credentials to a company's systems and who, one way or another, exceed their authority on the system and do something unauthorized such as sabotage servers or steal company data and sell it to a competitor.

But the true threat from insiders is a matter of debate with some experts saying the actual insider threats seen are small compared with today's external attacks. Then there is the question of how one defines an insider threat in the first place. Forrester Research, for example, defines an insider threat as any breach that is caused or facilitated by an insider, whether it is an "accidental insider or malicious insider," says Forrester Principal Analyst Joseph Blankenship. Forrester considers accidental insider attacks as ones where the insider had no malicious intent — perhaps an employee accidentally left a port open and an attacker leveraged that to gain access or saved a file to an insecure thumb drive so they could work at home rather than remain in the office.

Using Forrester's all-encompassing definition, Blankenship reports that insiders were responsible for 24 percent of all data breaches last year. But when limiting the definition to just malicious insiders — the definition commonly assumed in IT and security circles — that percentage drops to closer to 11 percent, he says. That suggests that 89 percent of all attackers were external.

"Some of the vendor marketing may be overblowing the insider threat," Blankenship says.

IDC uses a similar insider threat definition as does Forrester, also including unintentional

85%

Percentage of companies that will adopt cloud access security brokers by 2020

– Gartner

insider acts that facilitate external attacks. “The number goes down pretty dramatically if you start to remove things that are unintentional,” says Sean Pike, program vice president for security products at IDC. “Malicious is always a pretty small number, but they are very impactful because they have so much access.”

Another important component of an insider threat analytics strategy is whether to try and keep it secret or not. The “keep it secret” argument focuses on preventing any employee or contractor backlash from them being monitored so precisely. The “disclose it” argument speaks to deterrence, suggesting that the main reason for launching such analytics is less to catch insider evildoers than to discourage anyone from trying.

Indeed, the deterrence argument is made quite handedly by some companies that say that they are monitoring employees, when they really are not. Danny Rogers, the CEO of a Dark Web intelligence company called Terbium Labs, used to work with a casino that populated its money-counting rooms with fake cameras with little red lights on them. He calls it “security theater.” That way, the casino got almost all of the deterrence of true monitoring without almost any of the cost.

That works until an incident occurs and the company has to fess up publicly that it has no footage. But even then, would employees assume that all cameras are still fake? The cat-and-mouse game of loss prevention psychology will get a full workout.

Setting aside the psychodrama of “Are they or are they not tracking us,” the better question to ask is “Should they or shouldn’t they be tracking us?” Rogers positions himself in the “they shouldn’t” camp and he says it is for several reasons.

Danny Rogers, CEO, Terbium Labs

“When it comes to limits of mining employee data for signs of insider threats, I worry these efforts have already moved too quickly into the realm of ‘pre-crime,’ in which false positives result in employees’ benign activities being interpreted as threatening with employees being wrongfully terminated as a result,” Rogers says.

“The truth is that it’s very difficult to define ‘normal’ behavior for an employee,” he continues. “Often, one’s most productive and creative employees regularly engage in seemingly abnormal behavior as part of their work. In fact, onerous employee surveillance can have a chilling effect on innovation within a company. Generally, I think too much reliance on limited or biased AI (artificial intelligence), whether in looking for anomalous behavior of employees, software, or networks, is resulting in everything from alert fatigue to the increased risk of wrongful termination litigation. You have to have trust in the people in your organization.”

Rogers’ concerns here break down into two basic points. First, it is a bad idea to surveil because of where it might lead. Secondly, it most likely will not work anyway.

> “How great would it be to be the attacker who got in before your fancy baseline was established as the norm?”
>
> *– David Pearson, principal threat researcher, Awake Security*

As for why it likely would not work, Rogers’ argument is that deviation analytics, which is typically what machine learning does, needs to know what to look for. “You can’t really define abnormal until you define normal. Can you actually define a narrow

>33B

By 2023 more than 33 billion items of data will be stolen by cyber criminals

– Juniper Research

ring of normal for any given user?” Rogers asks. “It may sound nice in a marketing sense, but I don’t think you can define a narrow enough definition of normal for this to work.”

Rogers’s argument is that for the analytics to work well, it needs to be given a large number of samples of what network activity looks like when there are no insider attacks and it ideally also needs to be shown what it looks like when there are such insider attacks. But that is a challenge in logic, as a company would presumably never have complete confidence that there were no insider attacks happening during any sample period.

David Pearson, principal threat researcher at Awake Security, a former adjunct professor at the Rochester Institute of Technology and a member of the technical staff at Sandia National Laboratories, agrees with Rogers’ concern about the quality of the initial dataset. “How great would it be to be the attacker who got in before your fancy baseline was established as the norm?” Pearson asks rhetorically.

IDC’s Pike vehemently disagrees with both Pearson and Rogers. “It’s a little silly as an argument” that a company would never have a perfect snapshot in time of non-criminal activity, Pike says.

“You’ve got to start somewhere and you may very well need to start at a place where there is rampant fraud happening. As the system goes on, those behavioral patterns will change,” Pike says. “You might spot a pattern (of fraud) and go back and say ‘Now I see it.’”

Sean Pike, security products program vice president, IDC

Pike’s position is that companies must start by looking for the easy things, “the low-hanging fruit” such as employees logging in at odd times, starting to come in early or leaving late when that was never their pattern, their browsing activity, where they are logging in from, and which files are they trying to access. “It’s not so incredibly intrusive,” Pike says. “It’s sort of nonthreatening to employees.”

But is aggressive tracking an overall effective tactic to thwart insider attacks? Pike maintains that it generally is. First, there is a lot of monitoring that is required. “There are regulatory obligations to do some sorts of surveillance,” such as recording phone calls with customers, Pike says. Indeed, some surveillance “has been lifesaving,” such as when the system detects that an employee is acting suicidal.

> “I like my surveillance with a side of secrecy.”
>
> *– Sean Pike, security products program vice president, IDC*

As for employee pushback and potential resentment to extensive surveillance, Pike does not think that should be a significant concern. First, he does not believe that the surveillance should be announced. “I like my surveillance with a side of secrecy,” Pike says. “It really all depends on what you do with that information. The bad actors will probe ‘What can I get away with here?’ It’s only when you act on anything, that’s where you start alienating folk.”

For example, Pike says, if a manager cracked down on an employee for coming in late based on network analytics and cited the network analytics as the reason that could cause problems. It is better, Pike says, to file away such information and wait to observe corroborating evidence personally. “Even though you have the information, you don’t have to act on every single piece,” Pike says.

$13B

The encryption market is expected to grow from $4 billion in 2017 to $13 billion in 2020

– Researchandmarkets. com

Forrester’s Blankenship agrees. “How much are you advertising that you’re doing this monitoring? For example, has anyone been fired as a result? The employees may not even know that they are being monitored.”

Anton Chuvakin, research vice president, distinguished analyst, Gartner

Blankenship also points to the level of monitoring and how far it goes beyond what employees expect and assume companies are doing. And that perception changes sharply from one another with defense contractors and banking employees assuming far more surveillance than might be the case with agriculture and hotel industry employees.

“In the U.S., most employees would say that if they are working on a company device, that they would expect (monitoring) to happen,” Blankenship says.

Anton Chuvakin, a Gartner research vice president and distinguished analyst for security and risk management, says the attitudes about surveillance and analytics, especially as it comes to insider attack threats, sharply changes as the geographies and verticals change. “The European Union and Europe in general tend to be on the ‘do not do it’ side,” Chuvakin says. “The U.S. government does it a lot. And U.S. corporate is somewhere in the middle.”

Although Chuvakin offers questions about keystroke logging — “Is it creepy?” he quips — he stresses that the question is truly perceptional. “It is very heavily in the eye of the beholder.”

There is also a strategic question of how much time and effort should be focused on security dealing with the insider threat. For many in security, it is just not much of a priority. “People are too busy fighting malware to even think about insiders,” Chuvakin says.

When it comes to security and privacy, Europeans often look at the topic differently than their counterparts in North America. Catherine Flick is a member of the Association for Computing Machinery’s Committee on Professional Ethics as well as being a reader (the British rough equivalent of a tenured professor) in Computing and Social Responsibility in the Centre for Computing and Social Responsibility at De Montfort University, a public university in Leicester, England. She has strong feelings about privacy.

One of the never-ending problems associated with the European Union’s General Data Protection Regulation (GDPR) and copycat laws cropping up in North America, such as the California Consumer Privacy Act of 2018 on the ballot in November 2018, is that these regulations impose restrictions on what data can be retained and how it can be used. With analytics and employee monitoring, that simply increases how much sensitive data needs to be processed.

> “People are too busy fighting malware to even think about insiders.”
>
> *– Anton Chuvakin, research vice president, distinguished analyst, Gartner*

“There’s more than just the legal aspects of data analytics. Much of the law is still catching up. GDPR only just came into effect, and we’re still waiting to see what the real-world impact of much of that will be beyond annoying consent agreements on websites,” Flick says. “The [ACM’s] code [of ethics] has always had things to say about data privacy, security, and other ethical issues to do with analytics. Merging of datasets needs to be done with care to ensure privacy is protected; de-

10%

While 49% of British companies plan to increase investments in cybersecurity in 2018, only 10% plan to enhance data analytics

– Opinium Research

anonymization is bad [while] informed consent and user control over personal data is good."

Flick says she is inclined to think that aggressive employee monitoring for the purpose of thwarting insider security threats is "not an appropriate use of that technology" in general, although she adds that for some high-security businesses such as banks, "it might be appropriate." She argues it is better to focus on all security matters and "to trust (employees) and assume that they'll be professional. It's taking a sledgehammer to an ant situation."

Catherine Flick, member, Association for Computing Machinery's Committee on Professional Ethics; reader, De Montfort University (United Kingdom)

Flick notes that in the U.K., email and messaging communications cannot be examined by a company if it is explicitly labeled "union business." She adds: "It can have an overall negative impact (on business operations) if employees feel that they're not being trusted to do their job."

Pearson says the kind of analysis and monitoring that is typically dealing with insider threats can deliver far more headaches than it is worth.

"Decrypting and analyzing traffic makes it much easier to spot mal intent, but is also a great way to sow distrust with employees. When traffic is decrypted, it's an area that's ripe for abuse," Pearson says. "Obviously, knowing that somebody is searching Google is one thing, but knowing that and why they're searching for specific medical problems is something much different. Additionally, decryption offers another employee-focused crown jewel to any organization that does it. What if an attacker can access it?" he notes.

Pearson also argues that those kinds of employee-tracking techniques could undermine security if it drives employees to avoid such systems deliberately. "If knowing that the people controlling the analytics are seeing your private information causes you to actually engage in more risky practices, such as aiming to bypass a system by installing less trustworthy apps or using out-of-band devices, then the value of those analytics are significantly degraded," he says. "Instead, efforts should be made to find a more amenable approach, which may be analytics of intent associated with encrypted traffic without having to peek into the payload."

Doug Barbin, principal and cybersecurity practice leader at Schellman & Company, Inc., an independent security and privacy compliance assessor, talks about monitoring software that his company uses and how it works well, but mostly because his managers put limitations on it.

"Web monitoring software has been dancing this line for some time. Our firm, with almost entirely field-based professionals, uses a security proxy that protects our professionals from harmful networks and themselves. By default, it can see everything, even perform TLS (transport layer security) inspection of encrypted traffic," Barbin says. "Could we see employee connections to banking institutions or healthcare? Absolutely. Correspondence with potential employers? Certainly. But we don't and that is

> "It's taking a sledgehammer to an ant situation."
>
> *– Catherine Flick, member, Association for Computing Machinery's Committee on Professional Ethics; reader, De Montfort University (United Kingdom)*

90%

9 of 10 companies are vulnerable to insider attacks

– Crowd Research Partners

because we made a decision not to.”

Barbin points out that some verticals have non-security reasons for monitoring and it generates quite a few inappropriate incentives.

“In professional services, excess monitoring in such can cause you to miss context and flaws in the workflow. A manager could be penalized for projects going over budget, only to find out there was a project coding problem or the associate was incorrectly billing. Worse, firms have plenty of history of gaming chargeability and other metrics and/or asking associates not to bill all of their time to make project margins look better.

> “There is no easy answer other than good managers overseeing the analysts and asking why.”
>
> *– Doug Barbin, principal and cybersecurity practice leader, Schellman & Co.*

“Move out of consulting and look no further than healthcare where one treatment decision is made over another for the purpose of a better performance metric which drives funding and resources,” Barbin continues. “There is no easy answer other than good managers overseeing the analysts and asking why. Ethics professionals can also play a role going beyond their current mandate of privacy and protecting personal data to use of that data.”

Barbin also argues that metrics that some believe raise questions of improper conduct might signal nothing at all. “From an insider threat perspective policy scenarios, what are you monitoring for?” he asks. Do you disable USB thumb drives or transfers to certain web sites? For example, if an employee was sending files to Dropbox, would that not be a more worrisome situation? Perhaps or perhaps not, Barbin says. He notes that some of his clients post sensitive files on Dropbox if the file exceeds the size limitation of email, which makes lots of large files transfers to and from Dropbox non-suspicious.

Vast amounts of data moving today is not necessarily a bad sign at all. What if employees are just downloading a movie to watch at home that night? “I struggle where all of this wouldn’t be yet another instance of chasing your tail,” Barbin says.

For more information about eBooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an eBook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

#1

The most popular cybersecurity standard worldwide is ISO27001

– IT Governance