Teneo®

The Global CEO Advisory Firm

Teneo Insights

Insider Threats: How Do You Keep "Out" What Emerges from Within?

A discussion between Bill Bratton, Jonathan Wackrow and Steve Smith, senior members of Teneo's Risk Advisory team. Moderated by Kevin Kajiwara.

June 2019

Kevin Kajiwara (KK): I'm Kevin Kajiwara, Co-President of Teneo's Political Risk Advisory Practice. Today we are here to discuss an issue that all organizations face; exposure to and potential liability to an insider incident. I'm going to be speaking to several of my colleagues here to get to the bottom of what we mean by "insider threats" and how companies and their leadership can build security programs to deter, prevent, and mitigate against insider attacks.

To be clear, an insider threat is most simply defined as a security threat that originates from within the organization being attacked or targeted, often by an employee or officer of that organization or enterprise. Contractors, vendors, business associates, and other individuals who have knowledge of an organization's security practices, confidential information, or the assets the organization uses to protect their networks or databases all fall under the umbrella of insider threat targets.

Insider threats can also be described as a threat that cannot be prevented by traditional security measures that focus on (for example) preventing access to unauthorized networks from outside the organization or defending against traditional hacking methods.

And, unfortunately, the definition of insider threat has evolved to include destructive acts, such as physical harm towards others that happens in the workplace.

We're going to take a deeper dive into what deterring, preventing, and mitigating these various insider threats entails.

Commissioner Bratton, let me turn it over to you to frame the discussion, and to talk a bit about trust in the workforce and the implications when a trusted insider uses his or her access to do damage to the organization, either deliberately or unwittingly.

William Bratton (WB): Thank you, Kevin. The foundation to start building on is trust and I will focus specifically on the idea of bringing trusted employees into the company and then how you keep them, and how you keep them engaged in a trusting manner.

In terms of hiring of individuals to be brought into your company, organizations must trust their workforce. Let's face it, without trust, you can't survive. And particularly in today's networked world, the cyber world that we all exist in, the issue of trust is paramount. But with trust also comes verification. To gain trust, there must be a vetting process when you bring people into the organization; organizations really have to know

Bill Bratton
Executive Chairman, Risk Advisory
william.bratton@teneo.com

Jonathan Wackrow
Managing Director
jonathan.wackrow@teneo.com

Stephen Smith
Managing Director
steve.smith@teneo.com

Kevin Kajiwara
Co-President, Political Risk Advisory
kevin.kajiwara@teneo.com

who they are hiring. This part of the hiring process has improved dramatically over the years with the ability to have more extensive background screenings, but there are also new privacy laws and other legal limitations that present new challenges in this process. For example, in many states, it is now illegal for employers to ask about criminal history in a background check prior to hiring an employee or making an offer.

There's also, in today's 3% unemployment economy, the labor-shortage issue. In the current tight labor market, companies are more pressed to get employees hired quickly, so they take shortcuts on what would otherwise be an extensive vetting process.

Pressure to hire rapidly is a security risk that organizations have always struggled with. For example, in my former role in Miami, the Miami PD in the late 1980s had tremendous corruption scandals that came about as a direct result of the rush to hire hundreds of new officers to deal with the aftermath of the Mariel boat lift – the mass emigration of Cubans, who traveled from Cuba's Mariel Harbor to the United States. At this time, they quickly brought into the Miami PD many people who were not sufficiently vetted and the Miami PD ended up with some of the worst corruption scandals in American police history.

A more recent example is U.S. Customs and Border Protection, which has recently dramatically expanded their personnel to deal with the growing problems on the border, and one of the things they did to expedite the hiring process was to eliminate the lie detector tests. As a result, that agency has recently experienced significantly increased levels of corruption among employees, many of whom, if a vetting process had been conducted more thoroughly, would never have come into the organization in the first place.

Even with rigorous vetting processes in place, organizations face a variety of insider threats, including threats from rogue employees who deliberately cause harm by committing industrial and government sponsored espionage or workplace violence (which unfortunately, we see take place almost every day). There is also the issue of good employees who make mistakes, not intentionally, but that may be negligent about the kind of outside emails they open, or lapse on following company policies around use of email, sensitive information, etc.

With any of the above scenarios, the key to prevention and early detection is the development and nurturing of a secure, managed workforce as a risk mitigation practice including: fostering loyalty to the organization and its mission; team building exercises; and putting programs into place to create an informed, engaged workforce who understand the mission of the organization (and believe in it) and are willing to share the responsibility of protecting each other and the company.

Mitigating insider threats also requires a comprehensive, risk-focused program involving a wide range of stakeholders and operational areas, but should also strive for the proper balance between countering the threat and accomplishing the organization's mission and goals (and balancing the constant tension between those two opposite forces).

And lastly, the goal of an insider threat program is to detect anomalies as early as possible and investigate leads in order to interrupt the progression of potential insider threats before assets, data, or personnel are compromised. Post-9/11, many of us are familiar with the expression: "If you see something, say something," and while that term is most often associated with the idea of countering potential terrorist threats, it also

applies to the philosophy of mitigating and preventing the various insider threats found within companies, and really helps to simply sum up the idea of "we are all in this together" and reinforce the idea of a shared responsibility of everyone within an organization looking out for one another and the company.

So, companies need to give guidance and training to employees on what to watch for, and just as important, if they do see something of concern, how to report it.

KK: Thank you, Commissioner. We'd now like to drill down on the table you've set here. I gave a very cursory description of what an insider threat is, but let's get into that a little bit more and John, let me start with you, and your role at the Secret Service as part of the Presidential Protection Detail, your role as a financial crimes investigator, and the experience you've had in the private sector. You've seen pretty much the entire spectrum of threats in your career thus far. How would you define what is meant by an insider or internal threat, versus the more traditionally expected external threat?

Jonathan Wackrow (JW): What's really important for everyone to understand is that the insider threat is human-centric; it's people within the organization that pose the most serious type of threat. These individuals might be former employees, contractors or business associates - basically anybody that has a nexus or connectivity to the organization has the ability to potentially cause harm.

And I think what's really important is to understand the potentially devastating impact of this type of threat. Insiders can commit a variety of acts that inflict harm in any number of different ways, from the loss of information (data exfiltration) to physical harm within the workplace that the Commissioner alluded to earlier.

There are three different sub-categories that fall under the definition of an insider threat. The first is a malicious insider, somebody that has entered into an organization with the intent from inception to cause harm to either the organization's operations, financial well-being, or harm to the people.

The second is a trust-betrayer. The trust-betrayer is a long-time employee who has, over time, become disgruntled and as a result, lashes out; we've unfortunately seen many recent examples of this where people, over time, have become disgruntled either because of lack of promotion, or progress, or financial strain and then become violent within the workplace.

The third category, which is the most difficult to mitigate, is the unintentional insider threat. These are accidental acts done by employees that negatively affect an organization's systems or networks, usually resulting from negligence or just pure human error.

One of the keys to addressing these various insider threats is prevention. More specifically, prevention, deterrents and detection are the combination of mitigating factors that then lead to a well-informed and well-prepared workforce. And as the Commissioner mentioned earlier, the most effective organizational risk prevention programs are those where all members of an organization share the responsibility of that risk prevention.

KK: We all see examples of these events on the news every day, happening to someone else, but the reality of the situation is that it can happen to all of us. And what you've just talked about suggests that companies and organizations need an insider threat program - can you dive into that rationale a little bit further?

JW: When organizations analyze insider threat risk, they need to look at the numbers and they have to be able to quantify the potential impact. And financial impact should be a big driver around why organizations must be programmatic in their mitigation of insider threat. For example, if we just take a look at different data breaches that have occurred over the last couple years, where hackers have piggybacked on unsuspecting insiders, the numbers are pretty shocking. For example, the Yahoo! breach in 2016 effected 3 billion Yahoo! accounts; it was one of the largest breaches of all time. Another example is the 2017 Equifax breach, where over 147 million consumers had their financial information exposed.

In 2017, there were over 130 large-scale targeted data breaches in the U.S. and that number is growing exponentially year-over-year; last year we saw a 27% increase in data breaches. The loss of data is a huge issue for publicly-traded companies. And while not every breach can be traced to the actual insider, the majority have a link to the inside, either maliciously or inadvertently. As we keep mentioning, the most damaging security threats rarely originate from malicious outsiders; they most often come from the inside and are the result of a human-centric problem within an organization.

Another few statistics I think are important to mention: 90% of organizations surveyed feel vulnerable to the insider attack; 53% of organizations surveyed confirmed that insider attacks against their own organization have occurred within the last 12 months; and 86% of organizations have, or are building, an insider threat program.

These statistics all represent the greater trend that a majority of organizations feel vulnerable, but on the positive side, we are seeing movement with that number of 86% of organizations taking proactive steps to address these vulnerabilities.

KK: I'd like to hand it back over to the Commissioner to draw some parallels to the issues John just mentioned, specifically, outlining what the various police organizations you ran faced regarding insider threats and how they dealt with those threats and how you specifically dealt with it and the programs you put in place during your tenure at those various organizations.

WB: In both the business world, and in the world I spent most of my career in (the police world) when it comes to risk, the focus is on prevention; it has to be. The idea is to prevent to the best of your ability. But the reality is in the world of policing there are always going to be criminals, and in the world of business, there are always going to be issues such as John has described. So while a lot of the focus is on the prevention aspect of it, you also have to be prepared to respond.

Given this ever-present threat, there needs to be a laser focus within organizations on people, processes, and technology. And companies must not only have policies, but also training plans that support those policies. For those companies that don't have training (and constant training) on these policies, problems will inevitably present themselves. And these policies and trainings shouldn't just be focused on cybersecurity or

strictly the mandate of the IT department; health and well-being of the workforce should also be a priority. Organizations invest significant resources in their trusted workforce, so repair and rehabilitation are more cost-effective and risk-adverse options than waiting until it's too late for preventative measures and then trying to deal with disgruntled employees/disciplinary issues and the insider threat activity that it so often breeds.

When I was Commissioner of the NYPD, we put in place a program called "Are You Okay?". The goal of the program was to provide education and training to all 55,000 members of the department that if you see that there's something wrong with a partner, with a fellow employee, that the first step is something as simple as asking the question: "Are you okay?" This simple check-in served as a way for colleagues to support one another, look out for each other and the department, and also served as a great internal checks-and-balances system. This program is an example of the types of oversight mechanisms that the NYPD deployed internally to ensure that department employees were complying with significant policies and procedures that had been put into place, and to guard against police engaging in illegal activity - particularly as it related to the treatment of citizens.

The bottom line here is that all organizations need strong audit systems, monitoring systems and both internal and external risk mitigation programs.

KK: Steve, let me turn to you. Given your background as the former Threat Program Coordinator in the Bureau of Diplomatic Security at the U.S. State Department, can you share some specific examples of your experience with insider threats?

Stephen Smith (SS): I'd like to point out the three most infamous insider breaches that were the genesis for the government's focus on the insider threat issue.

I think most of the folks on the call are probably familiar with the terrible tragedy involving the Army Medical Corps Psychiatrist, Major Nidal Hasan. In 2009, he walked into his clinic in Fort Wood, Texas and fatally shot 13 people and wounded 32 others. This was an example of an insider threat incident that really changed how the Department of Defense thought about protecting their own workforce.

Another example is in 2010, when Corporal Chelsea Elizabeth Manning exfiltrated 750,000 documents containing classified and sensitive information from an army network, while stationed in Iraq, which she then sold to Wikileaks. That incident was the catalyst for the U.S. government to begin creating a government-wide insider threat program to monitor specialty classified networks.

The third example took place in 2013, when Edward Snowden, a National Security Agency (NSA) contractor, exfiltrated thousands of highly-classified reports on systems and programs and released those documents to the media.

KK: Considering all of those examples, especially on the Manning issue concerning the data breach, John, from a corporate perspective, can you touch upon the critical data that's vulnerable to an insider threat?

JW: I want to focus on two of the breaches that Steve mentioned. Back in 2010, when Chelsea Manning had the breach, and then again in 2013 with Snowden, I was at the White House. I was supporting the National Security Council in 2010 and was then on

the President's detail in 2013 during these two major critical breaches. At the moment when the government was trying to dissect exactly what happened, they didn't know what data that they had lost. They knew they had a breach. They knew they had information and files that were exfiltrated and now were out beyond the government's control, but they were really struggling with identifying what exactly had been stolen and what to do next. I make this point because organizations today need to identify the "crown jewels" of data that they want to protect long before there is a breach. And once those most critical data points are identified, organizations need to build a data governance policy around that, which puts in place a strategy for protection and management of that data within the organization. And each organization is going to have a different data set that they feel is the most critical to their business operations and reputation; some of those datasets might be confidential business information (financials, customer data, or employee data, etc.) or it might be sensitive personal information, such as healthcare information. And intellectual property is also often high on the list of a company's most valuable data assets, things like trade secrets, research, and products and design.

All of these things are different datasets that organizations have to take a look at and then prioritize. Company leadership need to ask themselves: "What are the organizations most critical crown jewels?", "How do we protect those valuable assets?" and "What type of governance structure do we put into place so that we are properly focusing our resources on protecting the right elements?"

KK: So we know what the problem is. We know that you need to do something about it. Steve, we're at the heart of the matter now. So how does an organization go about building a program?

SS: If you're a CEO, COO, or another key stakeholder in a company, you really "hold the keys to the kingdom," so to speak. And with that in mind, the first thing needed to properly build a risk management program is organizational buy-in and top-down support from senior leadership. Risk management is a holistic issue. It's a cultural shift to engage your workforce and send the message that "this is important" and "we are going to take this seriously," and "we're going to take the steps necessary to keep our workforce healthy and safe." It is a human issue. Building the right type of risk program calls for a very holistic approach. Organizations need to focus on their people and then focus on the processes and technology.

Another important component to the risk program is thorough insider threat identification. What and who are your company's biggest insider threats? And then, as John mentioned, you really have to put effort into defining your company's critical assets and analyzing tolerance for loss and damage. More specifically, defining your organization's critical assets and then putting measures in place so that you understand who is touching those assets - who has access, when they have access, and why they have access are all important things to keep track of.

Returning to my earlier point about stakeholders, you've got to get buy-in and participation from a very broad array of business units. You certainly need the legal team's support and participation. And HR is also a very significant player in the insider threat program, as they are the department with the finger on the pulse of a company's workforce; they understand if there have been any disciplinary issues or if there are going to be any dismissals or any other kind of people-related issues in the workforce. HR is also usually the team that runs an employee assistance program to support vulnerable workforce members. I would say that every successful corporation has an employee

assistance program to support with everything from mental health issues to financial issues. Having a system in place so that companies can engage with and support employees before they become an insider threat is important.

And on the point of engagement, making it easier for the workforce to engage is very important. And by engagement, I don't mean reporting or snitching. This type of engagement is more about people taking an interest in their colleagues and their company and understanding when some members of their workforce are vulnerable. Anonymity is important with these kinds of programs, as a lot of people don't like to raise their hand and be someone to report on a colleague. But again, it's part of culture change. It's about engagement for the better of the whole. And there are a lot of safety communication platforms out there that can provide the technology to support these programs and provide the anonymity necessary for these programs to be successful.

So involving all the right internal players in policy building, training programs, and organizational change management is paramount to the development of a sound risk management program.

KK: John, at the outset, you gave an interesting stat, which suggested that an impressive, but not sufficient, percentage of organizations are implementing these programs. What are the barriers that companies find to building a program?

JW: The number we cited earlier, that 86% of organizations surveyed said that they are trying to build some sort of insider threat program, is certainly an impressive one, but when we look at that number and dissect it a little bit more, we don't know what type of program they're building. Is it something that's based in IT only? Or is it an enterprise model that looks at all of the different threat vectors from an insider that can affect the organization?

So although that 86% number is a good one, we have to look at what the barriers are to actually implementing a comprehensive program. And when we start talking about the barriers to building a program, it starts at the top because the senior level buy-in of an organization sets the tone. Unfortunately, a lot of people view an insider threat program as bringing forth a solution to a problem that doesn't exist; a lot of senior leadership within an organization don't want to accept the fact that they could have a trusted betrayer within the organization. So instead of taking a proactive approach, they take a defensive posture to say, "Well, that's not going to happen here." And that's a barrier to success for any type of program. I have heard on a couple occasions senior leadership at various organizations say things like, "Hey, we haven't had a breach yet so we don't have to put this mitigation plan into effect," and that's just the wrong strategy. So organizations, once they do get that all-important senior-level buy-in, have to decide what their strategic insider threat program is going to look like.

Earlier in the call, the Commissioner gave examples of insider threat programs built on a trust-based approach. But there's also a new model right now that a lot of companies, especially on the IT side, are adopting, which is the zero-trust model, which is trust nobody and don't give anybody access, whether it's around their physical access to buildings or access into certain critical systems. And I think that zero-trust approach is another barrier.

Once the organization does decide what type of strategy they're going to go with to address the problem of the insider threat, they next have to look at all of the implications that come along with it, including the issue of institutionalized bias within an organization, and whether certain policies and procedures related to the insider threat program in any way cause bias towards one particular group within an organization. So programmatically, when you start wire diagramming any type of insider threat program, you also have to decide if your strategy matches the culture of your organization, or will it limit, or potentially alienate, members of your organization. And there really isn't any off-the-shelf solution for building an insider threat program because every organization is different and has different objectives, so you have to match in a measured way what type of insider threat program you want to introduce.

KK: I think on one of the other critical elements that a management team is always going to want to protect, though, is corporate culture, right? So how do you protect collaboration, open sharing of information and all of those things that make an organization a vital and dynamic one? And how do you prevent it from becoming a culture of, to use a blunt term, a bunch of snitches essentially? How do you prevent that from happening when you're rolling out the types of programs that you're talking about?

JW: I think that when you talk about corporate culture, again, the tone is set from the top. The senior leadership team needs to establish an environment where people are encouraged to share information because at the end of the day, all employees are stakeholders. And as such, they have a collective responsibility to support and contribute to creating an environment of security awareness.

Senior leadership also needs to encourage various pathways for employees to be able to report information anonymously, in advance of any type of incident, whether it's data exfiltration or some type of violent act. And as Steve mentioned earlier, there are a lot of different technological platforms that are out there that actually make this an almost seamless process.

No one wants to feel that there's a potential threat within their organization. So people should be encouraged to share information in such a way that it becomes part of the ecosystem instead of outlier behavior, where people are deemed as a snitch or a tattle tale and ostracized for it. It's about establishing a culture that supports and values a safe and secure environment.

Teneo

Teneo is the global CEO advisory firm.

Working exclusively with the CEOs and senior executives of the world's leading companies, Teneo provides strategic counsel across their full range of key objectives and issues. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other global corporations.

Integrating the disciplines of strategic communications, investor relations, digital advisory, diversity & inclusion, management consulting, physical & cyber risk advisory, financial advisory, corporate governance advisory, political risk advisory, and talent advisory, Teneo solves for the most complex business challenges and opportunities.

teneo.com