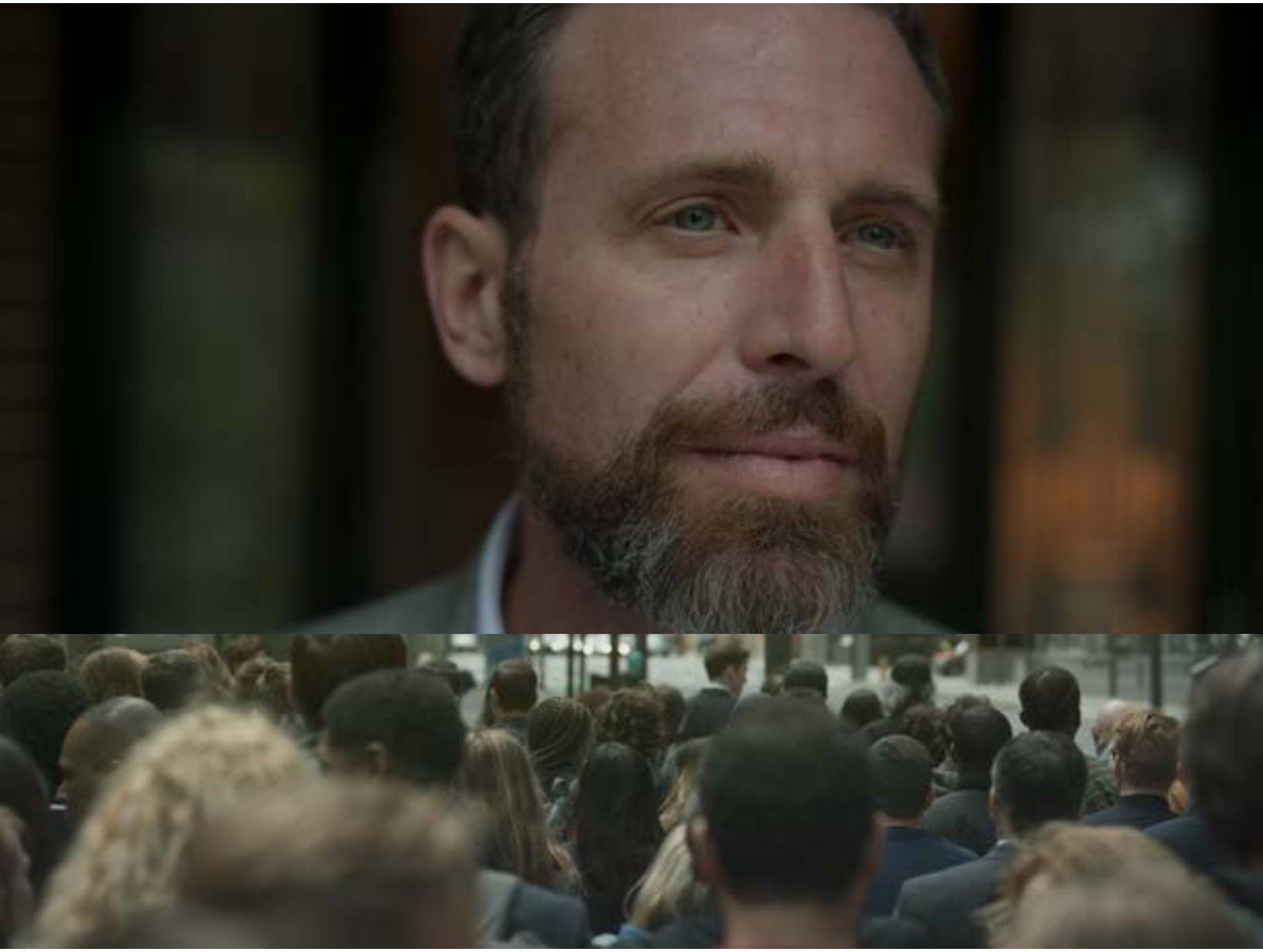


CISO INSIGHTS: 7 BEST PRACTICES FOR A SUCCESSFUL INSIDER THREAT PROGRAM

15 CISOs from FORTUNE 200 companies met at Forcepoint's 2017 Executive Advisory Board (EAB) meeting, where we explored ways in which CISOs can help enterprise insider threat programs deliver on their promised results.

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

FORCEPOINT EXECUTIVE ADVISORY BOARD MEMBERS

- **3M:** John Valente
- **ACCENTURE:** Andy Vautier
- **AT&T:** Karthik Swarnam
- **DARDEN RESTAURANTS:** Scott McBee
- **DISCOVER FINANCIAL SERVICES:** James McJunkin
- **KELLOGG:** Tim Bengson
- **MARKEL CORPORATION:** Patricia Titus
- **MGM:** Scott Howitt
- **MONSANTO COMPANY:** Gary Harbison
- **RAYTHEON:** Jeff Brown
- **REALOGY HOLDING CORPORATION:** Nashira Layade
- **REGIONS FINANCIAL:** Jeff Kennedy
- **ROSS STORES:** Elwin Wong
- **U.S. BANK:** Jason Witty

Introduction

Organizations face a litany of challenges as they build modern security programs designed to combat the advanced and sophisticated threats of today. Among them, one of the most complex lies in the area of "insider threat." Beginning with the term itself, insider threat presents a new set of obstacles, ranging from process to policy (including privacy) to technology to functional partnerships across the enterprise.

Importantly, companies approach insider threat in a variety of ways. Some focus specifically on employees or contractors (more literally "inside" the enterprise); others broaden the definition to incorporate individuals whose identities have been compromised by another person, or malware impersonating a human being. There is not one right answer, but addressing insider threat in some fashion is important, because failing to do so may have a material impact on the organization.

Given the complexities associated with insider threat, Forcepoint convened our Executive Advisory Board to take a deep look at the issues they face, and the collective recommendations this group might put forth for others to consider. In this CISO Insight brief, we share 7 best practices as identified and agreed upon by a group of FORTUNE 200 cybersecurity leaders.

In Forcepoint's Executive Advisory Board (EAB) meeting, 15 CISOs identified some practical steps that may help remedy some of the challenges many of us experience when developing and implementing an insider threat program.

We agree that, often, insider threat programs are not as effective as they should be or need to be. There are some very simple and valid reasons for this. With a focus on detecting malware threats and meeting compliance demands, enterprises have done too little with their insider threat programs to actually reduce the risk of data loss. And as CISOs, too often we've overlooked the most obvious risk – our people - who mostly just want to get their job done but, at times, inadvertently expose critical data.

It's important to keep in mind that we're all on this journey together. This is a process of discovery and understanding and is certainly not intended to be the last word on the subject. But we believe that the best practices outlined in this brief can help get our insider threat programs working the way we need them to, which will help all of us do our jobs more effectively.

BEST PRACTICE #1

Consider the "why"

As CISOs, it's important that we think critically about what leads to insider threats. A key piece of understanding the "why" is identifying the intent of behavior, and many on the EAB do this by defining specific categories of insiders. One EAB member, for example, categorizes insiders into one of four buckets: inadvertent, intentional, malicious and state-sponsored (a subset of malicious). By defining insiders in this manner, it enables this CISO to more clearly identify the intent behind the incident.

Another member shared that when it comes to insiders, the majority of incidents are related to employees taking documents (such as PowerPoint presentations) on to their next job. Interestingly, this is rarely done in the context of industrial espionage or competitive attacks. In fact, it's much more personal than that – people are simply looking to leverage templates and approaches that have proven successful as they enter into their next assignment.

BEST PRACTICE #2

Adapt language to culture and audience

Some of us found that using the term "insider threat" to name the program was an obstacle in itself when it came to employee acceptance of the program. In addition, some EAB members found that our peers on the executive team may react negatively to the term. As one member noted, "When we start talking about insider threat, right away they correlate that to us saying our employees are being bad and we have bad people working for us."

That's completely understandable. Who wants to be labeled as "an insider threat?" Besides, it's not necessarily the most accurate description of what the program aims to accomplish. An insider is anyone with access to our data – an employee, a privileged user, a third party contractor or an outsider who has stolen credentials from any of the above.

"Terminology we use, such as 'insider threat,' can chip away at trust," said Patricia Titus of Markel Corporation. And, we need the trust of our employees. After all, the first line of defense is an individual sitting on an endpoint."

To avoid any potential stigma, some CISOs have opted for renaming their insider threat programs. "Employee Protection Program" and "User Protection Program" are two examples, but there are certainly other alternatives. For example, instead of a name with potentially negative implications, some may choose one that acknowledges the real relationship between our employees and our data. Yes, our critical data is valuable, but it's our employees who scale that value. Without them, our data sits in a vault and we have no business, no customers nor market share. Our data and employees are our "core assets" and are worth protecting. With that in mind, a name such as "Core Asset Protection Program" might make sense.

For others, the program name isn't the problem, but rather, how the program is communicated to employees.

The reality is that some level of monitoring is necessary to protect our employees, critical business data and IP. But how many of us really want to freely sign up to additional monitoring in our work or personal lives? It can be much more helpful to approach it from a human perspective.

The bottom line is that every CISO should think carefully about their company culture, and what they choose to call their program should align with that culture. While it may seem trivial, getting the name right is an important first step in setting the tone of what we are trying to accomplish for our employees and businesses.

BEST PRACTICE #3

Present the program as a partnership

We believe that ultimately, data protection begins and ends with our people. An effective insider threat program focuses on the human aspect of security. This makes perfect sense since both data and human security – protecting our core assets–are really the same thing.

"Everyone universally understands why we need to protect the data – to protect the company," said Nashira Layade of Realogy Holdings Corporation.

What might this partnership look and feel like?

Begin by treating our employees like partners. Let them know just how important they are: we're trusting them with the company's most critical data and trade secrets. We shouldn't underplay this fact. Our company's existence and future is literally in their hands each and every day. Overall, the theme of transparency must be resident in any insider threat program: the EAB believes we must be open, honest and clear about what behaviors we are monitoring – and why.

Next, we should let them know that accidental human behavior is the major factor for failure in all systems - not just in cybersecurity. We should also highlight the fact that compromised and malicious insiders are outliers, not the norm. Explain that because of this, and the fact that the frequency and complexity of data breaches are exploding, safeguards must be put in place. The probabilities and risks are just too high not to do so. We must be sure to stress, however, that we're not pointing any fingers. Human error–whether accessing unsafe cloud apps to get a job done faster or simply clicking on a targeted phishing lure–is the biggest cause of data breaches, from the C-suite on down.

Beyond partnering with employees at large, we also believe that functional partnerships will be critical to the success of any insider threat program. One EAB member, for example, noted the critical role of partnering with the company's audit and compliance executives. Another identified the role of human resources as a critical partner, given the potential impact that an insider threat may have on employees.

In summary, insider threat programs cannot be addressed in an IT or cybersecurity vacuum: they must be built in partnership with the company's employee base, executive team and board of directors.

> "Everyone universally understands why we need to protect the data – to protect the company." — Nashira Layade, Realogy Holdings Corporation

In order to define how that partnership works on a day-to-day basis, our user-focused insider threat program (or whatever name you wish to give it) between the enterprise and our people needs specific guidelines and processes in place. For example, letting our people know precisely which activities will be monitored is a good start. Also, let them know which activities will not be monitored or stored. We'll also want to establish a process for our employees to elevate concerns safely and privately, and what data and workplace privacy rights they have. In other words, clear guidance and transparency will make for a successful enterprise-employee partnership.

From this human-centric perspective, we've found that an effective insider threat program helps us:

- **understand how our people interact with our valuable data**
- **analyze that behavior for risk**
- **guide our users to make smarter decisions with data**

That's why truly effective data security is really about understanding human behavior so that our employees can make the best decisions and take the most responsible actions.

BEST PRACTICE #4

Focus on the positive outcomes

But monitoring is just a part of the "how–it doesn't convey the real benefits that we all realize from the program. In presenting an insider threat program to our organizations, we should focus on the positive outcomes, the additional security and protection that it brings. In doing so, we need to let our employees know that the program protects them and the company's critical data (the enterprise's core assets), the enterprise's reputation, and of course, the employees' jobs, healthcare, retirement plans and families.

In other words, this program can and should be a win-win. For our companies, we are protecting our assets and intellectual property; it's the lifeblood of our organizations and critical to our business. This also has a direct impact on employees: our organizations will be better positioned to be more competitive, meet our growth targets and win in our markets if we protect ourselves.

BEST PRACTICE #5

Prioritize the role of culture

Every insider threat program's effectiveness is highly dependent upon employee support. This is one of the difficult parts of deploying a successful program because it involves changing people's attitudes and behaviors. That doesn't just happen; it must be instituted and reinforced over time.

One EAB member shared their company's experience that brought this point to life. For nearly 30 years, the member's organization has focused on a culture that frowns on added bureaucracy. At face value, this sounds like a wise approach. But, as insider threat programs are rolled out, process and policy build. This fundamental conflict launched a debate about the company's culture and led to the decision to rethink some engrained norms due to the reality of today's threat environment.

This real life example poses a very practical but crucial question for all of us: "How much time and effort have we spent presenting and enforcing our insider threat program to our employees?"

In most cases, the answer is, "not enough."

Successfully standing up an insider threat program involves a transition period, ongoing training, honest engagement and transparency with our employees, in order to build the trust and comfort level throughout the enterprise. Everyone should see the need and the benefits of the new program. We should let our employees know and feel that we're all in the process of adopting the program together. In effect, insider threat programs involve a long term relational evolution with our employees that will become embedded in our culture. The new policies should become a part of the on-boarding process for new employees as well.

BEST PRACTICE #6

Align around executive and board responsibility

Protecting our people and our critical data relies directly on executive responsibility. Any effective insider threat program must have deep executive support in a very visual, obvious and even celebrated way. Without full participation from the top down, the odds for success fall dramatically.

The chances of getting (and keeping) executive support can be improved by focusing on the positive outcomes – we start with a defined list of use cases and then expand it over time. We can begin by explaining how protecting our people is the most powerful means we can leverage to protect our data. For example, one of our EAB members noted that they began their insider threat program by first solving for PCI compliance and then built it out from there.

In some cases, garnering executive support may begin in the C-suite; in others, the mandate may come from the board of directors itself. If the board is driving the decision, we may need to educate the members in order to avoid the risk of framing the intent or scope of the program to only malicious insiders. Such a narrow focus will miss the larger purpose and limit effectiveness of the program. The real and ongoing benefit of the program is to discover compromises and identify poor security hygiene throughout the enterprise.

Regardless of where the advocacy for an insider threat program begins, we believe that building a metrics-based story is critical to making the business case for investing in the people, process and technology necessary. The executive teams and boards operate largely by evaluating data; insider threat programs must be addressed with the same level of quantitative rigor.

As one EAB member stated: "When I can get the metrics to support the case for an insider threat program, they will understand it more."

In addition, the EAB agrees that a regular cadence of both executive and board-level communication is necessary. One member shared that threats are covered at the board level during each directors meeting (four or five times per year). In addition, the topic is covered at the senior vice president level and above once per month. The point is, regardless of the cadence you choose, do make a choice and follow through on it. Consistency is key to keeping the topic front-and-center.

With the appropriate tools, policies and support in our insider threat programs, we may see results that are eye-opening.

For instance, we may find compromised credentials, someone using our servers to generate Bitcoin or an employee on their way out of the company stealing massive amounts of data. We will definitely identify more accidental use cases than we otherwise would. At that point, our executives will need to decide what they're going to do with these results.

What's the appropriate governance structures that allows us to respond and take action?

A comprehensive, executive-endorsed response plan is also part of an effective insider threat program. We agreed that deploying and implementing a successful insider threat program – or whatever we choose to call it–is a top-down, policy-driven process that involves investing in the right tools, creating new procedures and responses, and instituting new cultural norms throughout the enterprise.

> "When I can get the metrics to support the case for an insider threat program, they will understand more" — FORCEPOINT EAB Member

BEST PRACTICE #7

Focus technology investments on the outliers

We all agree that technology is only one piece of the puzzle; insider threat programs involve people, processes, policy and technology. But from a technology standpoint, we do believe in the need to focus and think differently. Specifically, it's about identifying the outlier behaviors that raise red flags.

"We are trying to look differently at the insider threat problem, and use technology in innovative ways as part of our programs," said James McJunkin of Discover Financial Services. "It's the alternative to boiling the ocean. Instead of looking at everything, focus on the linkages that should not exist in order to identify real threats."

Overall, the EAB agrees that understanding the behavioral norms of an individual user on a day to day basis is a critical capability within an insider threat program. By establishing baseline behavior, only unusual user activities need be the focus.

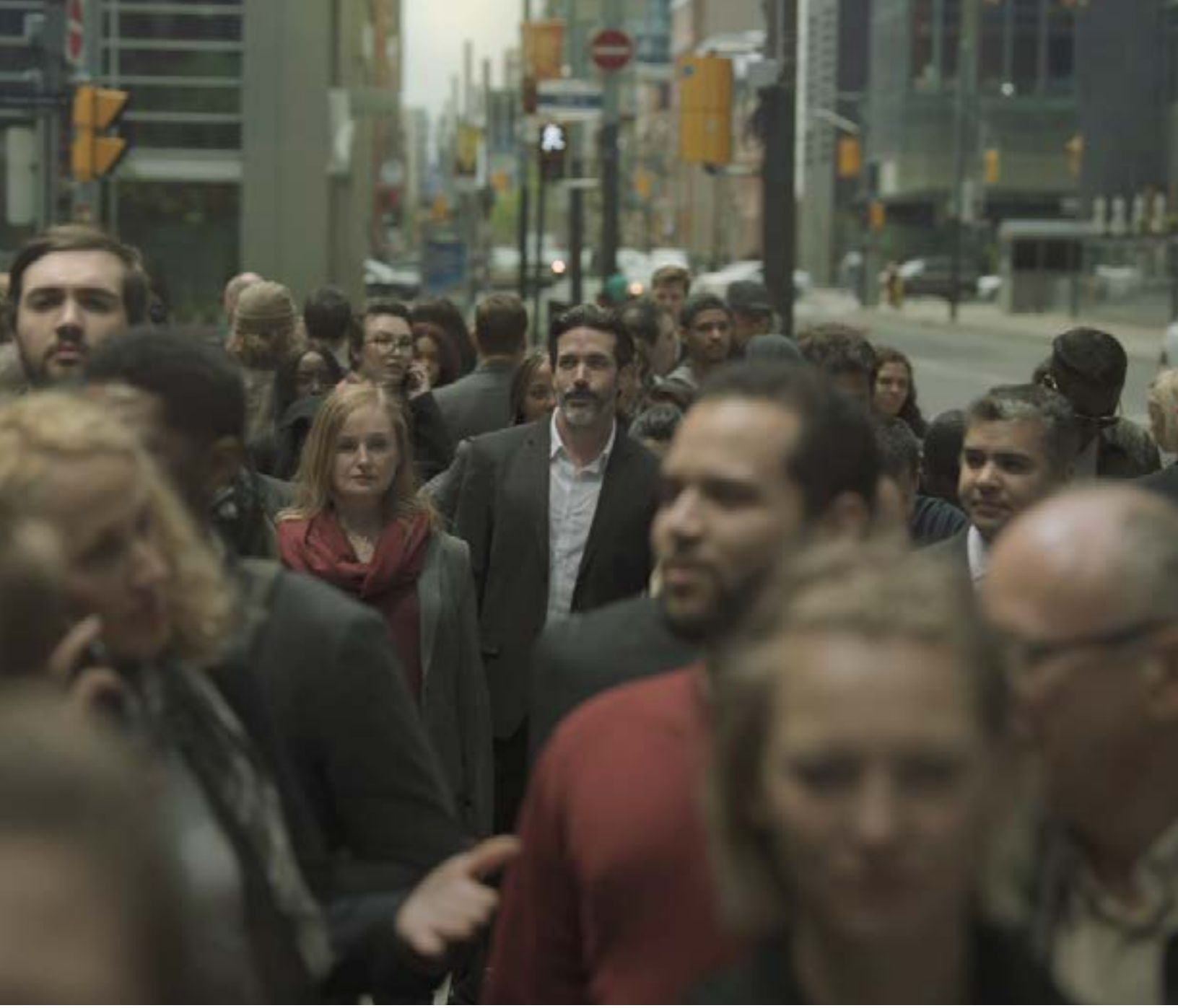
"You can tell when a user has swapped out – it's the style of the individual and how they behave. As you're monitoring the style – what changed?," said Patricia Titus of Markel Corporation.

"In an insider threat program, you're looking for strange behaviors that are not normal for an employee – be it because someone else is using his or her credentials, or because the employee may be doing something accidental or malicious," said Gary Harbison of Monsanto Company.

We also believe the role of forensics is vital in any insider threat program. Because these programs look at behaviors, the first set of data simply provides a view into what occurred without understanding the why. Answering the why will get at the root of the problem – whether it was an employee who made a simple mistake, acted maliciously, is a victim of compromised credentials, or a host of other possible reasons. The point is, we must look beyond behavior to understand the intent.

Finally, we concluded that standing up and maintaining an effective insider threat program really isn't an option for enterprises any more– it's a necessity. Doing it right is an ongoing process and requires effort and persistence. Furthermore, we have no doubt that more requirements and program aspects will become necessary in the future. But if we're not able or willing to take these seven steps today, our insider threat programs are likely to remain ones in name only.

> "In an insider threat program, you're looking for strange behaviors that are not normal for an employee – be it because someone else is using his or her credentials, or because the employee may be doing something accidental or malicious," — Gary Harbison, Monsanto Company



ABOUT FORCEPOINT

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit **www.forcepoint.com** and follow us on Twitter at **@ForcepointSec**.

CONTACT

www.forcepoint.com/contact