SECURE|ANCHOR

AN INTERVIEW WITH DR. ERIC COLE ON

# INSIDER THREAT

# HOW MUCH OF A PROBLEM IS INSIDER THREAT?

When I work with organizations on cybersecurity issues, I sometimes feel like I'm Paul Revere: essentially I run through organizations and scream, *"The insider is coming! The insider is coming!"*

But maybe it's better to say, *"The insider is already here."* Because when I talk with executives, it amazes me that insider threat causes so much damage to organizations—yet it's the area that many organizations are ignoring, or aren't even aware of. One of the problems is that when executives think of an insider threat, they think of a malicious insider, someone who deliberately causes harm to an organization. While that is a concern, the bigger concern to an organization is what I call the accidental insider threat. This is someone who is tricked or manipulated into doing harm without even realizing it.

# WHY DOES EXTERNAL THREAT GET MORE ATTENTION?

I think part of the problem is the media focusing on and hyping the external threat that's out there.

If you turn on the news, if you open a newspaper, if you read a magazine... you hear about all these external threats. You can pick your favorite country. You can pick your favorite organized crime group. The media is always covering how they're targeting and going after organizations.

It's not the media's fault, though. External threats get so much coverage because there's a visible component that's hard to ignore. The problem that everyone misses is that while the source of many threats is external, the reason they get in is because they are targeting an insider and using that as the point of entry to set up a pivot point.

If someone takes down or defaces your website; if somebody takes your private information and posts it out on the internet; if bad actors do a denial of service attack against your organization; if your organization loses a critical amount of regulated information and you must disclose it publicly... It's hard to deny those things. It's hard to ignore them. They make for good news, so the media pursues those stories.

However, it is important to remember that in almost all of these cases the insider played a role—and the more damage, the more significant a role the insider played.

But here's the problem with the insider threat: in many cases, there's nothing visible about it—because it's the people who are already in your organization that have access and who are doing the harm.

# SO IT'S NOT ABOUT *"BREAKING IN,"* LIKE MANY EXECUTIVES THINK, IS IT?

The insider threat is not about *"breaking in."* The people harming you aren't necessarily even doing things they're not supposed to do.

They're simply using your information in a way that's not intended to cause harm to your organization, either deliberately or accidentally.

In most cases, the insider does not intend to do harm, but is tricked or manipulated by an adversary. I often joke with people that APT does not stand for Advanced Persistent Threat; it stands for *"Average Phishing Technique."* Because in many cases it is just a well-crafted email that looks legitimate. If you receive an email from your boss or colleague with legitimate content related to a project you are working on, there is a very high probability you will open the attachment or click on the link. Adversaries know this and will spend time doing reconnaissance to make the malicious communication seem as legitimate as possible.

That's why I call insider threat the silent killer. In many cases, by the time you realize it's there, the damage is already done.

Your employees already have access—you're giving them access to data to do their job. But they're using that access in a way that you did not intend.

That means bad actors are not breaking in. They're not violating any security. They're not going to be blocked by your firewalls. And you're not going to be alerted, because this is access that you gave your employees, and those employees have been compromised.

# HOW DO YOU COMBAT THAT?

If you're not looking in the right area, if you don't have proper visibility, you just won't be able to go in and solve the right problems.

One of my mantras is *"let data drive decisions, not emotions."* It's easy to get emotional about the data and assets for which you're responsible.

But I always tell executives to step back and ask themselves, *"What is the data showing us? What are the problem areas we really need to be focused on?"* One of my favorite sayings is: Smart people know the right answer; brilliant people ask the right questions. Are you asking the right questions when it comes to insider threat?

In my experience, the biggest problem with insider threat is that most organizations just don't have proper visibility. They don't know what their employees are doing, or what their contractors are doing. They don't have any data—and therefore, they don't have any idea if they have a problem.

Here are a few quick wins you can implement right away: control attachments coming into the organization, know where your critical data is, and properly manage access control.

Most damage by an insider is caused by the user being tricked into opening an attachment or clicking a link. I am a big fan of awareness, but awareness will not help in this case. An organization must remove the vector by blocking or properly verifying attachments and web links from the internet.

In addition, most users have more access than what they need to do their jobs. Controlling and limiting access can go a long way toward minimizing the damage caused by an insider.

# WHERE SHOULD EXECUTIVES START?

Where's the first place to start? Begin by asking questions and having your security and IT team provide data on the insider threat in your organization. The big focus needs to be on controlling access and controlling the damage. While executives need to focus on strategy and not tactical decisions, having the right strategic metrics around the problem and solution is a good place to start.

Are people accessing information that they shouldn't? Do you see large amounts of information being copied to USB drives? Any unusual or strange activity? Are people installing programs that they shouldn't? Are people connected to websites? Are people turning off their end-port security?

Answers to these questions will give you insight into what's happening—and whether you really have an insider threat problem.

# WHAT IF YOU FIND YOU HAVE A PROBLEM?

Remember the data you used to get visibility into the problem? You can also use it to measure whether you're really fixing your issues.

Knowing that you have a problem is one thing. If you have the same problem 12 months from now, or it's worse than it was, then clearly the security measures you put in place aren't working or aren't focused on the correct area.

I often get frustrated with how organizations throw money at business solutions without tracking metrics to see if they're doing the right things, so they can concentrate on what really matters and make adjustments if they find themselves off-course.

Have the data. Get the metrics. Gain visibility into what's really happening in your organization and how bad the problem is. And always remember that the goal of security is not to prevent all attacks, but instead to control the overall damage caused by an attack.

# DO YOU SEE A LOT OF INSIDER THREAT ISSUES?

Having worked with organizations of all sizes, I have never—ever—found one that doesn't have an insider threat problem.

I'm often tempted to simply tell executives, *"I guarantee you'll have a problem,"* but it's often easier to let the data make that case for me. I don't want people to take my word for it; I want them to look at what's really happening.

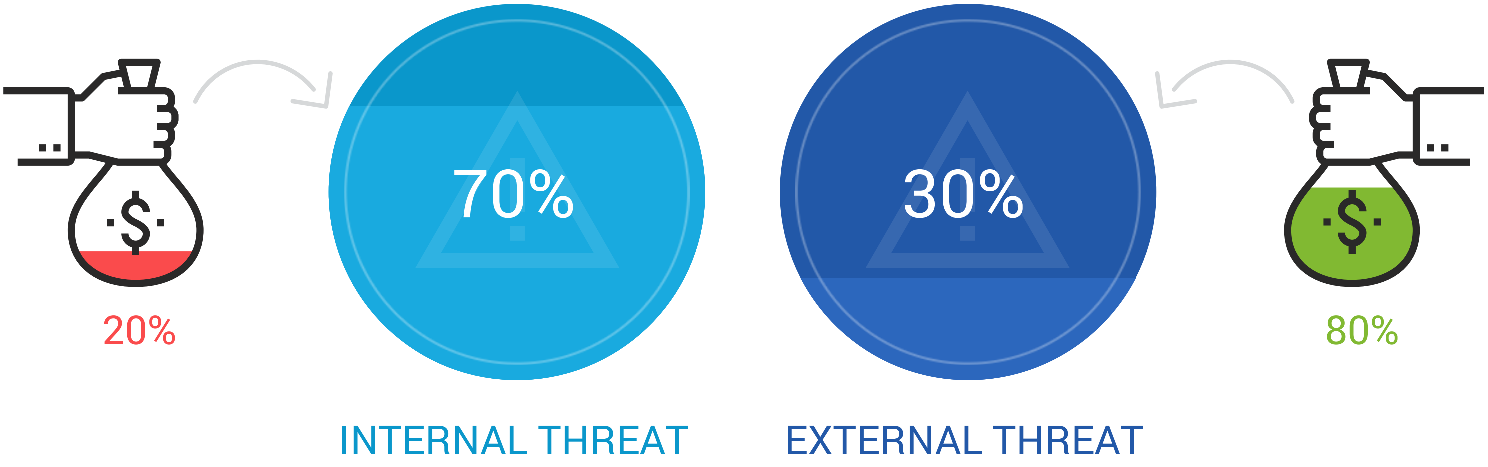
When my clients and I start looking at exposures—and we do root cause analysis of incidents and damage—we typically find that only about 30% of the incidents and related damage is coming from external threats.

In other words, more than 70% of the damage, exposure, and impact to the organization is actually coming from insiders.

The problem with many organizations is that they are not looking in the right place and performing proper assessments. That's equivalent to saying you are healthy even though you never go to the doctor or get a physical. You could very well have problems that you are not aware of.

Unfortunately, this is the approach most organizations take with insider threat, but ignorance is not bliss. They think if they do not acknowledge it or look for it, it will go away—but clearly that is one of the biggest mistakes an organization can make.

# HOW SHOULD I ALLOCATE MY BUDGET FOR INSIDER THREAT?



I'm not saying you shouldn't spend money on internal and external threats. But many of my clients typically spend about 80% of their budget on external, and only about 20% on internal—if that. Sometimes it's even less.

What does your budget look like? Are you spending 80% on something that's only causing 30% of the problem? Let data drive decisions. Calculate what percent of the damage is being caused by the insider and properly align your budget.

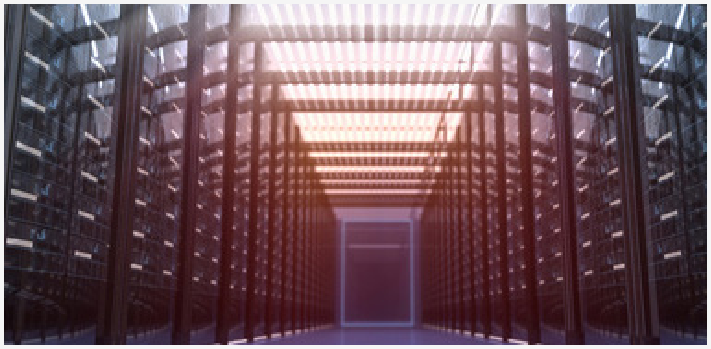
Sometimes I get pushback from executives who say, "If you look at all the news and media, it's all talking about external, external, external." But you have to differentiate between the source of the problem and the cause of damage.

In many cases, yes—the sources of many attacks are external. However, the cause of damage is more likely an insider.

Yes, occasionally you see a traditional attack where someone tries to hack your servers. However, that's becoming harder and harder to do because organizations are getting better at addressing and fixing those problems.

ten years ago, what was the easiest, most effective way of getting into a system? Finding a server with a public IP address, identifying services via ports that were vulnerable and not patched, and using that to break in.

And what did many organizations do in response? Focus their energy on hardening, locking down, and doing asset inventory. Many of my clients have their DMZ systems very secure, very protected, very patched and very hard to break into; however, they fail to realize that via email and web-based activity attackers can use insiders to access the client systems that tend to be more vulnerable.



# SO WHERE DOES THE INSIDER THREAT COME FROM?

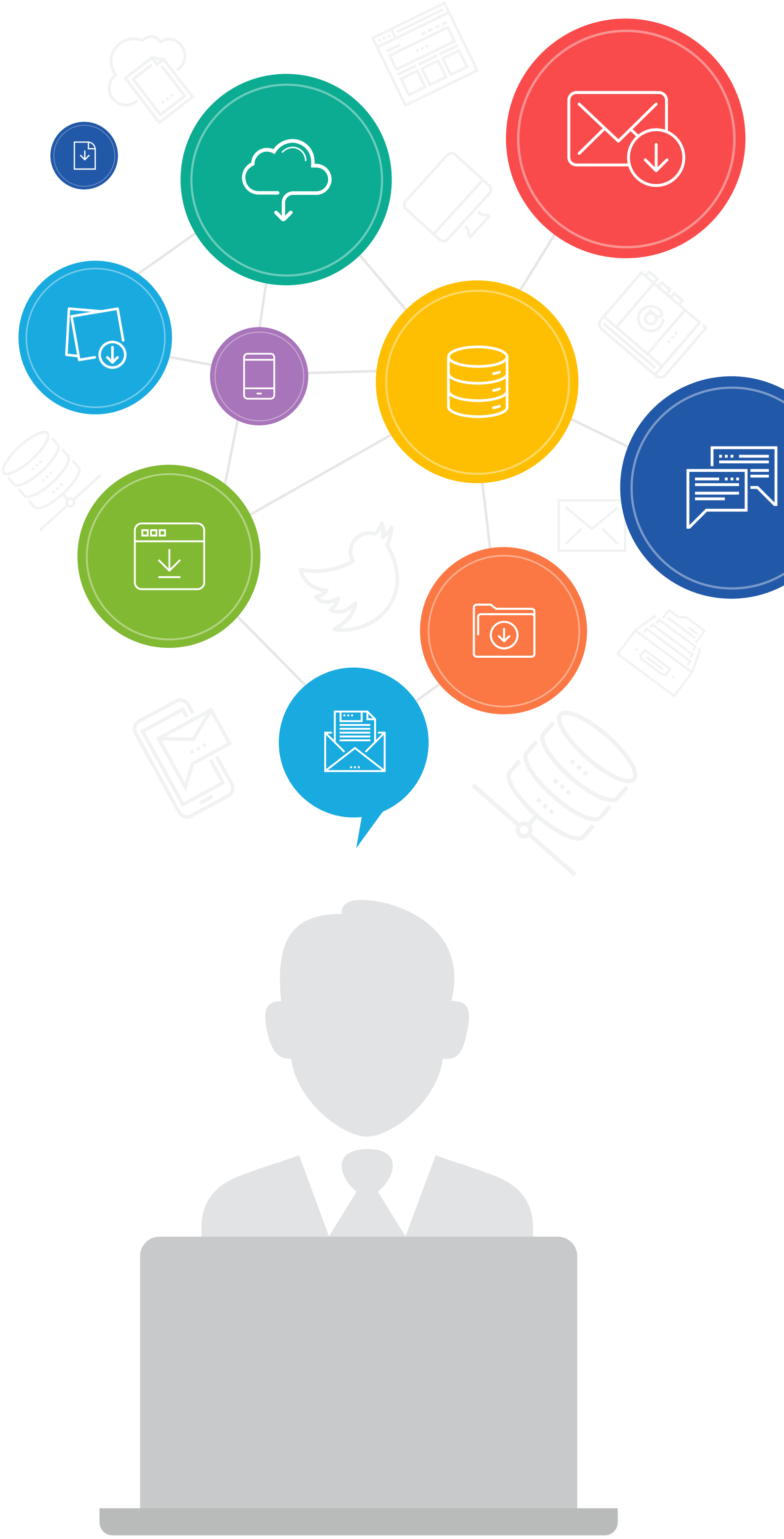
So now you have adversaries saying, *"How do we get in? How do we get the information that we want?"* Then they realize, *"Wait a second. Let's target someone who's already inside. We can pay them, blackmail them, or recruit them to be a deliberate, malicious insider."*

Now that works, but it costs money and takes time. So then the adversary asks, *"Why am I paying somebody within the organization to help us when we can trick people into doing it for free? If we go in and we look at the information out there about them, and we understand their job and their corporate structure, we can craft communication that looks legitimate and trick them into doing the work for us."*

And when your employee receives an email and it looks like it came from their boss or a customer or a colleague, when the content is good and the name of the attachment is valid, and when the information inside looks legitimate—they don't even realize they've been targeted.

That's why I'm so confident that this problem will get worse until it gets better.

What I'm seeing now is that it's much, much easier to target somebody within the organization and get them to give adversaries access to the organization. They're targeting employees with legitimate looking emails, with executables or web links that look and feel legitimate. And as an industry we're not fixing it.



# WHY DOES THE INSIDER THREAT REMAIN UNADDRESSED?

We're focusing all our effort on the external—and the more secure we make the external, the easier it is for them to keep targeting that insider threat. And I think budgets need to be adjusted accordingly.

So yes, the biggest concern for you today is the accidental insider—somebody who's a good employee who doesn't want to cause harm.

They don't want to cause damage, but they are tricked or manipulated into doing something they ordinarily wouldn't do.

Question: how many people, if they received an email that they honestly believed came from someone they trusted, would open that email? If you're saying *"no one,"* I have a question for you—does your family know you lie?

Look at the diverse range of technical knowledge at your organization and your answer is going to be at least double digits, and possibly in the high double digits.

You may vet your employees, or do background checks. You may think you have trusted, loyal employees who are never going deliberately and maliciously cause harm to your organization.

That may be true, but your biggest problem is the accidental, unintentional insider that can be tricked or manipulated.

# IS THE PROBLEM BIGGER THAN A LOT OF EXECUTIVES THINK?

Fifty-three percent of organizations say they've experienced an insider incident. And in my opinion that number is very low, because many organizations do not have proper detection measures in place.

Why? Because most of them don't realize they have an insider threat until two to three years after they've been compromised. The reason comes back to visibility—many businesses just don't have monitoring tools, and so aren't able to track anomalies and identify unusual or suspicious activity.

Once again I want to ask you a question. Does your current security allow you to find somebody within your organization whose system is compromised and slowly leaking sensitive information in email-encrypted form? What about someone copying information to a USB or a cloud share or an encrypted drive and then copying it when they get on their home computer? Are you going to be able to see that unusual activity and be able to take action and deal with it?

If you don't have mechanisms and measures in place to find insider threats, you need them. Thirty-three percent of organizations have no formal response plan... How about yours?

**Get the data. Ask the questions. Look at what's happening.** Look at where the gaps are. Ask yourself if those gaps are or are not acceptable for you to have an appropriate level of security. **And take action.**

# IS THERE ANYTHING THAT CAN BE DONE?

This isn't a hopeless situation—it's simply that new problems require new solutions.

At the risk of repeating myself, you need to start with getting visibility into what's happening. Build profiles and baselines, and then look for anomalies. Look for strange or unusual activities. Perform insider threat hunting. Instead of being on the defense, go on the offense and aggressively look for the compromised insiders and take action.

Yes, some of your employees are going to have different patterns of behavior, but just because somebody has some anomalous activity doesn't mean they're automatically a threat.

If you have 80,000 employees in your organization and I tell you that 5% of them are insider threats, that doesn't help you because you can't monitor thousands and thousands of people.

But if you focus on looking for those anomalies and find 45 people out of those 80,000, you just got rid of a lot of straw in your search for the needle in the haystack.

You can then take a closer look. Maybe they're good employees and are just anomalies. Or maybe their systems or accounts have been compromised, or maybe they are actually bad actors.

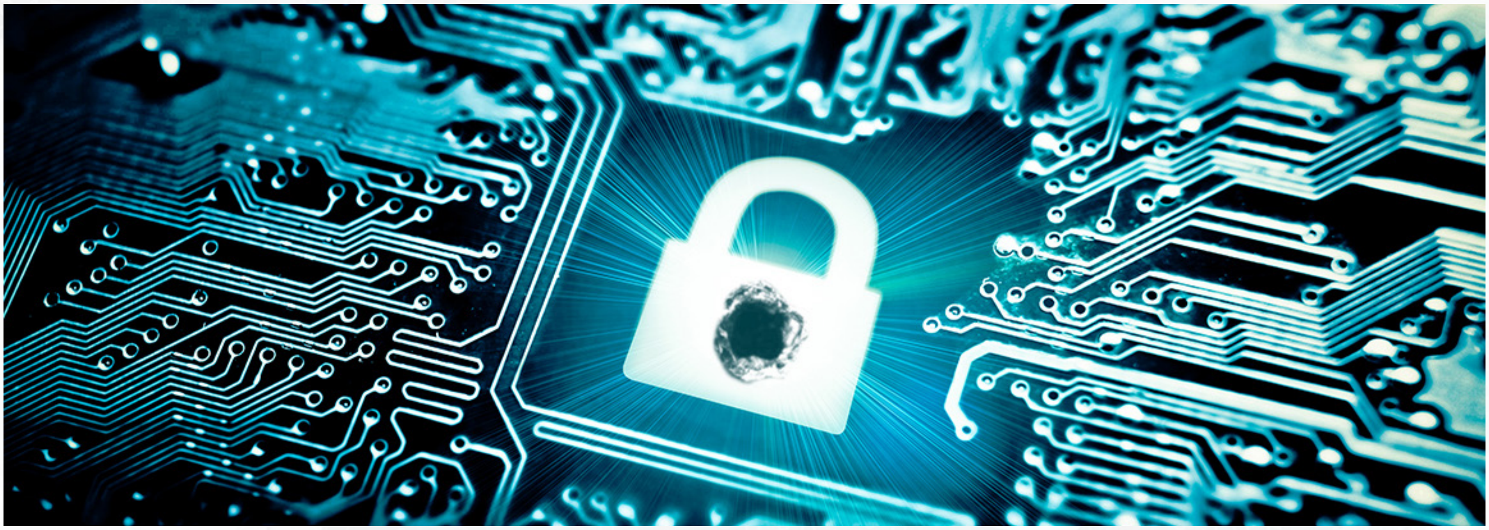
# ARE FALSE POSITIVES A PROBLEM?

Yes, you'll get false positives. I once built an insider threat program for a large government contractor; we had 37 indicators and I flagged on 17 of them. According to most rational descriptions, I myself could have been considered an insider threat.

However, I told them, *"Look at me. I'm proof that you need to monitor, evaluate, and verify."* Because those indicators by themselves, in my case, showed there might have been a problem. But obviously when you evaluated and verified, I checked out because I was just doing my work as head of security.

The important thing to remember is this—finding the insider threat is about correlating activities. It's not about any one single data point. Any individual's going to have anomalies—it's how you find the ones that rise to the top that makes the difference.

# WHAT WOULD YOU RECOMMEND TO AN ORGANIZATION LOOKING TO GET STARTED?



First, ask yourself what information an adversary would target. What critical information—if it was exposed, destroyed, or altered—would damage your reputation as an organization?

Where is that data stored? What systems does that data reside on? Who has access to that information?

Are you monitoring that access? Are you looking for anomalies? Are you tracking and tracing who actually needs that access and has that access?

I recommend a process called threat modeling, where you're trying to think how an adversary would work.

It's simple to do. Take a piece of paper and break it down into three columns.

Start in the right column with a list of your critical information, and what systems or servers it resides on.

Then fill the left column with a list of threats that have the highest likelihood of causing harm to your critical data, and the things that could happen that would allow that information to be exposed.

Finally in the middle column, list your vulnerabilities. For example, *"We don't have monitoring,"* or *"Anybody can add any access,"* or *"We're not monitoring or removing access."*

Once you've listed your vulnerabilities, start to connect the dots. Start to model how an adversary could target insiders to cause harm.

You'll end up with a better picture of which threat would need which vulnerabilities to cause data loss, and which data would be vulnerable. And you'll find that not only will you start to understand how an adversary could work, but you'll also start seeing where the gaps are in your current security.

If you're lucky, you'll also see *"the kingpin vulnerability"*—not necessarily your top vulnerability, but the one that—when you consider risk, and threat, and access to critical information—could cause the most damage.

When you're done, you'll have a great picture of where your gaps are. What are the areas where you don't have enough visibility? What are the areas an adversary could cause harm without you preventing or detecting it? Then you can start building out a security road map that's closely tied to insider threat.

# AREN'T SOME PEOPLE JUST BOUND AND DETERMINED TO DAMAGE YOU?

Yes, some people are just evil. Their whole intent for getting hired at your company is to cause harm. This fails under the category of malicious insider, such as an Edward Snowden. The trick in these cases is to control the damage by limiting the access that any one person has.

But most people aren't. So ask yourself: what would cause a good employee to go bad?

They don't get a promotion. They're going through a messy divorce and need money. They're being harassed by a co-worker. All of these things could be tipping points that you need to identify and mitigate, because you can prevent a lot of problems simply by keeping employees from "tipping."

Let's say they do tip, though. They're then going to start searching for data and information that they can use to cause harm. Which means if you see significant changes in access behavior or users—for example, if they're trying to access more information, or they're trying to go after projects that they don't need to access, or they're trying to set up more accounts or more passwords—you need to look at the anomaly.

Remember, however—not every insider threat is malicious. So when you look at the unintentional insider, typically you're going to see certain behaviors: opening executables in emails, clicking on web links, plugging in USBs, and so on. In those cases, you'll see a whole flurry of activity that occurs on their behalf that's quite different than anything they've ever been doing.

But once again, with proper monitoring, the accidental insider can be detected and caught. You're going to see an inflation of back door programs, or new network connections, or a lot of very suspicious, unusual activity.

# WHAT’S A GOOD FIRST STEP FOR AN ORGANIZATION THAT WANTS THE *“LAY OF THE LAND”* AROUND INSIDER THREAT?

Ask yourself... Do you have clear, effective policies that talk about insider threat or address it? Do you have proper procedures that show the steps your employees have to take? Are you providing proper training so they have the skills they need? Do you have the proper metrics in place? Are you controlling access to data? Do you have proper segmentation to control and limit the overall damage?

Focus on policy, training, and awareness. Policy tells employees what to do. Training gives them the skills for doing it. Awareness changes behaviors so your employees do what they should.

However, as with any solution, combating insider threat requires an integrated approach. A product is not, by itself, going to protect you. Training, by itself, is not going to protect you. It’s all the pieces together. You need to have clear policies that people understand and recognize those dangers. You then need technological solutions to monitor and detect anomalous behavior. And you need to be able to assess the risk to your environment.

Going forward, make sure you’re always doing some kind of insider threat hunting. Recognize you’re going to be a target—the probability that you have insider threats in your organization is as close to 100% as you can get.

Go in and start looking and saying, “Do we already have compromises?” Start looking at damage assessments. Do you have exposures that already exist?

Remember, visibility and metrics are critical. If you cannot measure it, you cannot manage it. You’re not going to be able to catch and find adversaries if you’re not watching and tracking what users are doing. As soon as you get that visibility, you can start to track the anomalies, investigate, and limit and control the overall damage—both what’s already occurred and what’s to come.

# INSIDER THREAT?

## CONTACT THE EXPERTS

If you'd like to learn more about insider threat and how to combat it in your organization, consider Secure Anchor Consulting.

A worldwide leader in information security services for public and private enterprises, Secure Anchor Consulting has the experience and expertise to keep your personal and corporate property where it belongs: in your hands and under your control.

### About Dr. Eric Cole

Eric Cole, PhD, is an industry-recognized security expert with over 20 years of hands-on experience in consulting, training, public speaking, and expert witness testimony. As the founder and CEO of Secure Anchor Consulting, Dr. Cole helps clients prevent security breaches, detect network intrusions, and respond to advanced threats.

SECURE|ANCHOR

☎ 703.675.2055 ✉ info@secure-anchor.com www.secureanchor.com