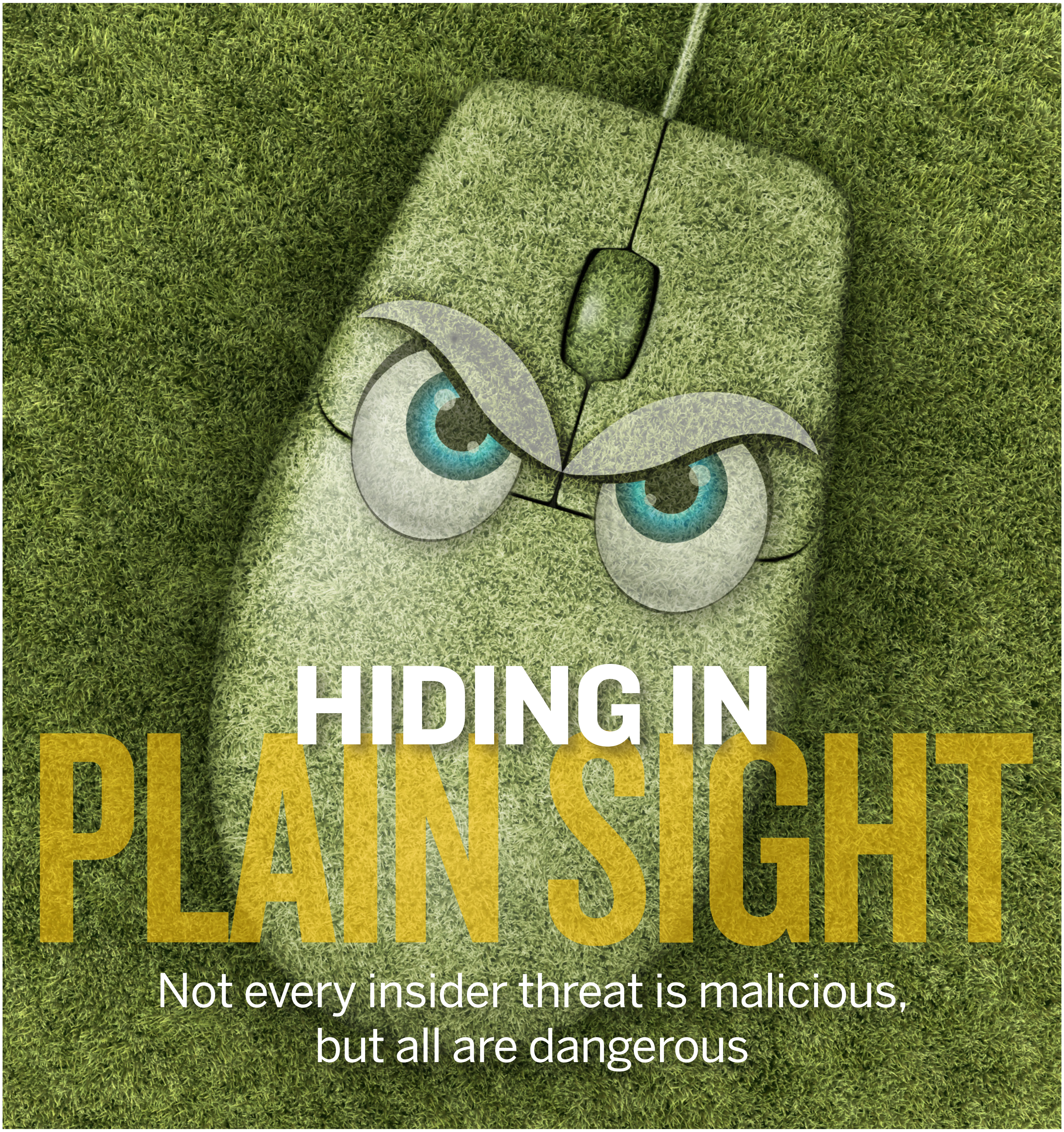


HIDING IN PLAIN SIGHT

Not every insider threat is malicious, but all are dangerous

ebook
An SC Media publication

Sponsored by

ARCTIC WOLF

FORCEPOINT

wombat™ security
a division of proofpoint.

Transgressions within

No one likes to admit it but insider threats are among the most serious companies face. Distinguishing the malicious from accidental is challenging, especially as attackers become more sophisticated. Jesse Staniforth reports.

As companies fall victim to increased insider threats, one of the greatest casualties has become trust in coworkers. Where one used to think primarily about threats to network security as coming from external intruders, today CISOs need to contend with the increasing likelihood that the threat actor might be a colleague — perhaps someone close to the IT staff, a disgruntled executive or other employees, a contractor or maybe just someone trying to do their job. Sometimes the threat actors are not even aware that they are doing anything wrong.

In light of recent, high-profile breaches, it might well be getting easier to convince the C-Suite to take threats from within more seriously. In 2018, insider threats have become one of the most pressing worries at a time when executive management across many industries is finally realizing the potential enormity of security breaches. That awareness, though, comes at the cost of attacks that are only increasing in scale and complexity. Securing against insider threat is a process that requires immediate attention. That said, companies are still trying to sort out what is a real threat and what is just an employee doing their work.

OUR EXPERTS: Insider Threats

Robert J. Hudock, member, Epstein Becker & Green P.C.

Eric B. Levine, co-chair, Cybersecurity & Data Privacy Group, Lindabury, McCormick, Estabrook & Cooper P.C.

Gavin Mead, Principal in Cyber Security Services, KPMG LLP

Robert Olson, technical director, Rochester Institute of Technology Security Assessment and Forensic Examination Lab

Richard Rushing, CISO Mobility, Motorola

Billy Spears, CISO and SVP, loanDepot

The non-malicious insider — perhaps the employee who downloads a confidential file to a thumb drive to work on it at home — might or might not be aware they are violating security policies. Sometimes the pressure of getting a job done on time takes precedence over an obscure security policy if the company is not proactive in training staff about what is and is not an acceptable use of resources. Sometimes it is just easier to ignore the rules for efficiency's sake.

Robert Olson, technical director of the Rochester Institute of Technology Security Assessment and Forensic Examination Lab, begins his investigations of insider threats using threat modeling designed to profile potential attackers by understanding their malicious motivations.

"The two models I point [students] at are MICE (money, ideology, coercion, and ego) and RASCLS (reciprocation, authority, scarcity, commitment, linking, and social proof)," he explains, noting that these detailed explorations of what motivates spies and attackers have become standard in the CIA and other investigative circles.

Olson argues that regardless of the attacker, a lack of strictly enforced organizational policies plays into adversaries' hands. "Insider threats are only possible when employees can access confidential or proprietary information or systems with impunity," he says. "Organizations with strong access control policies, which are enforced with technical controls that also monitor for violations, should be reasonably resilient to attacks from insiders."

Eric B. Levine, co-chair of the Cybersecurity & Data Privacy Group for

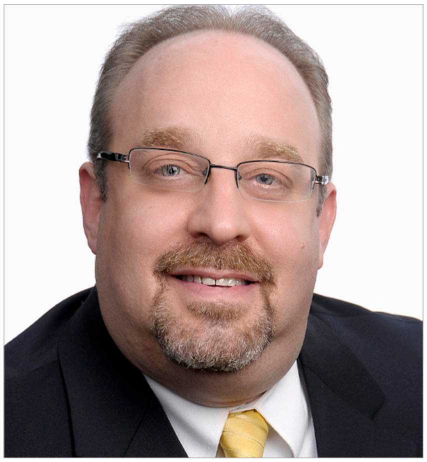
50

Average number of days to resolve a malicious insider attack

– Accenture 2017 Cost of Cyber Crime Study

Lindabury, McCormick, Estabrook & Cooper P.C., a Westfield New Jersey law firm that works primarily with closely held companies and their executives, focuses primarily on the rogue employee when he thinks of the most pressing insider threats.

Levine identifies rogue insiders as "those insiders who are unhappy with the organization, seem disgruntled and appear poised to leave." He cautions security people to take notice of insiders who engage in unexpected activity on the network, such as downloading large numbers of files. "These are warning signs that your organization's data may be subject to an unauthorized access."



Eric B. Levine, co-chair, cybersecurity & data privacy group, Lindabury, McCormick, Estabrook & Cooper P.C

Motorola Mobility CISO Richard Rushing agrees with Levine, noting that the insider threat is one best identified early through close consultation with human resources. Rushing says that if he can get copies of employees' performance reviews, it provides a fast track to being able to identify potential insider dangers.

> "People who are on a work-improvement plan or a needs-improvement plan are probably the biggest risk for insider threat"
>
> – *Richard Rushing, CISO Mobility, Motorola*

"People who are on a work-improvement plan or a needs-improvement plan are probably the biggest risk for insider threat," he says. But if HR will not share those documents, it is a matter of using the tools you have in front of you to assess how workers seem to feel about the organization, and how they express those feelings in actions, as evidenced by time and attendance records or badge access passes logged in the security information and event management (SIEM) system to show who is coming to work on time and staying the whole day.

Considering the quandary of insider threats, Robert J. Hudock, a member of Washington, D.C., law firm Epstein Becker Green, recalls a quotation from Russian Nobel Prize winner Aleksandr Solzhenitsyn's *Gulag Archipelago*, who wrote: "The line dividing good and evil cuts through the heart of every human being. And who is willing to destroy a piece of his own heart?" That is the challenge every organization faces, he says.

An employee who today might never have considered stealing data might reconsider tomorrow when he gets a pink slip, while a disgruntled employee thinking about how she could profit from her access to data may be brought back on board the team tomorrow with the right encouragement. What matters, Hudock says, is understanding that both types of employees are equally dangerous at different times in their careers.

"The blind spot for many organizations here is the realization that anyone can become an insider threat to an organization," he notes, "so it is in the best interest of all to implement an effective insider threat program."

Aside from the malicious insider and outsider, one threat actor who hangs in that gray area between the two is the employee who is being laid off and want to take their work with them when they go, Rushing notes. This might not be a deliberate malicious attack; instead it might simply be an employee who wants to keep copies of

40%

Percentage of survey respondents who reported malicious insider attacks, up from 35%

– Accenture 2017 Cost of Cyber Crime Study

their work without the intension of harming their employer deliberately.

"Whether it be source code, marketing presentations, customer lists, or anything else," he says, "people are just taking their stuff. They figure, 'I'll grab my documents and email and all those things, copy it to my USB drive and walk out the door with it.'"

Rushing stresses that the majority of these people likely do not see what they are doing as exfiltration. However, when they find a new job working for the competition, they discover they have migrated to the new company with a portion of their former employer's confidential data.

They are not acting with malice, he says, but "They maybe need to be reminded of this during the process and told, 'Hey, you really shouldn't be taking things that are company specific.'"

Another prominent form of insider threat actor is the wholly unwitting one, entirely unmotivated by any goal. Gavin Mead, principal in KPMG LLP's Cyber Security Services, explains, "Unwitting insiders are now equipped with capacities and opportunities to do inadvertent harm on a more frequent basis, from posting sensitive materials to cloud storage, to wrongly sharing sensitive data with suppliers, to using information in a way that violates regulation, to enabling an outside attacker to take over their credentials."

Richard Rushing, CISO mobility, Motorola

The rise of third-party logical and physical access to data, networks, and facilities — whether contractors, vendors, or contingent labor — concerns Mead, who notes that because they are less known, vetted, and monitored, they present an even bigger risk than employees.

Mead says that there is a tendency to focus too much on the malicious insider and as a result, organizational problems might neglect the potential harm of the unwitting actor, though a well-crafted program for defending against insider threat should contain provisions for confronting both eventualities.

The Data

Unwitting insiders vex loanDepot CISO and Senior Vice President Billy Spears. "Organizations should be concerned about insiders that are unaware of appropriate requirements," Spears says. "These are folks that want to do the right thing, and definitely are policy followers, but have a business need to use or share information without guidance on the appropriate methods to safeguard this data."

Spears notes that this group is the biggest problem because they cannot be readily detected, require additional training, and almost never think about data safeguards as they go about their daily business. For that reason, he says, once- or twice-a-year training is insufficient.

"That never really keeps the risks fresh or top of mind," Spears warns. "I think it is important to communicate at the level of your audience via an appropriate channel that makes sense. This is something that needs to happen weekly to assure that people understand what to do if they recognize a risk or need advice."

Ultimately, it is up to the security and IT teams, as well as the owners of the business data, to ensure that confidential data is not only protected but that it also is clearly identified. If the company does not know what data it has, what level of confidentiality it requires and how it is protected, it is difficult to ensure that it will not be exfiltrated, accidentally or otherwise.

"It is critical that an organization consider and understand what types of data might be vulnerable to attack in order to understand the

90%

Percentage of companies that say they are vulnerable to insider threats

– Crowd Research Partners

implications of responding to unauthorized accesses of that information and how to prevent such access from occurring," Levine says. He notes regulations like *Health Insurance Portability and Accountability Act (HIPAA)* or the *Gramm Leach Bliley Act* help organizations understand what information must be protected.

Of course, he says, organizations are presented with the challenge of determining which classes of their information are protected by law. However, they also must protect valuable data not subject to regulation.

"An organization should assume that all of its data is vulnerable," Levine says. "Whether the data is personally identifiable information, protected health information, or something more general like a client list, a company should assume that some third party may find some improper use for obtaining that information. The better approach is to build your defense around all of your data."

Mead says that the first step of any insider threat program is determining a formal definition of the organization's business drivers and its crown jewels.

"When taking a threat-driven risk scenario approach, understanding the data at risk is a critical consideration," he explains. "This includes assets and information as well as business functions that are at risk: moving money, changing reporting structures, creating new employees and changing employee direct deposit information, destroying production capability, damaging reputation and others."

Gavin Mead, Principal, cyber security services, KPMG LLP

However, he says, it is tricky to tighten access to data without becoming unnecessarily restrictive — and a restrictive attitude can strike at the values of team collaboration necessary to protecting data.

"While restricting access to some data is a strong control, it is critical for an organization to understand the spread of sensitive data and of privileged access," says Mead. "The failure to understand what constitutes sensitive data, failure to manage sensitive access and review its appropriateness, and the constantly-changing nature of peoples' jobs and technology enablement leads to access drift over time."

Managing The Data

Rushing is a proponent of establishing a high standard for granular-level access control because those who cannot access the data cannot remove it or transfer it where it does not belong. This is a nearly end-to-end process; it is not enough to mandate it but it needs to be enforced continually.

Like all good ideas, Rushing says, access control starts out pristine, but once it is left to wither, it can cause problems. "It has to be a continual environment," he says. "There's some level of responsibility you want to bestow upon whoever's the custodial person responsible for managing that data, and you really want to empower them to make decisions."

Classification, he says, is a key element of prevention. Footers, headers, and metatags allow CISOs to track data that has turned up where it should not be, where it has been, and how it is moving around the organization.

"If there's nothing in it then it becomes really hard for any [tracking] to actually work," Rushing says. "If you know where all your data are and the repositories of your data are, you then have an idea of here's what I need to protect. If you haven't gone there yet, it's like boiling the ocean."

One reason so many organizations allow

53%

Percentage of respondents who said they were victims of an insider attack in 2017

– Crowd Research Partners

too much access is simple convenience, says Levine. Securing sensitive company information is initially time-consuming to classify the data. It also requires time to authenticate the users each time they want to access the data. A compounding problem in organizations occurs when there is no clear record of what data they have, where it is stored, and who has access to it, he notes.

Billy Spears, CISO and SVP, loanDepot

"Organizations need to adopt practices that provide that they secure all data upon its creation or initial acquisition, meaning that the files are secured, password protected or accessible only to limited people who have authorized credentials," Levine says. "Organizations also need to invest the time and resources to map their data in order to learn what data they possess, where on their computer network the data is located, and who can access it. Investing the time and resources at the upfront and then adopting it as a routine practice is a substantial undertaking, but one that will create a more secure environment on an on-going basis."

(Much of what Levine says about protecting data became mandated on May 25 if the data contains private information about European citizens. That was the day the European Union's General Data Protection Regulation (GDPR) went into effect. Among its requirements is knowing exactly where data on EU citizens resides on the network, on every corporate or personal device, and in every backup or archive, regardless of where in the world the data resides.)

However, the process of recording all this information is a complex project, says Olson, who notes that lax security is rarely due to laziness on the part of system administrators, network administrators, or programmers.

"Time and financial constraints make [security] a challenge for many organizations," he says, and the problems become exacerbated by organizational cultures that allow such constraints to spread. "If respect for data privacy isn't baked into strategic security policies set at the executive level, technical controls preventing unauthorized — or unethically authorized — access will receive less or little priority and employees are less likely to protect data privacy in day-to-day activities."

Even conscientious staff members can engage in risky behaviours, such as cloud-based file-storage, when they have not been properly prepared to adhere to rules and best practices while still running the business effectively.

"Once this mentality sets in, monitoring for malicious behavior becomes even more difficult, as it is often comingled with innocently motivated, but still out-of-policy actions," Mead says. "Insider threat programs have to work to be positively perceived by the employees they monitor. Employees must understand that the program is designed to protect everyone's job and livelihood and not perceive it as 'Big Brother' driven by employer mistrust. Programs that fail to create this positive perception with employees can actually be the cause of disgruntlement, becoming part of the problem they are attempting to solve."

The Program

The way an insider-threat program portions out its defenses to detection, deterrence, and post-breach forensics is determined by what kind of data it is defending.

Rather than counsel for a percentage split on each approach, Rushing says it is better to keep asking questions of the data: "How do I track it? How do I see it in transit? How do I trust it at a third party or anything else that's doing something with it? What kind of controls can

53%

Percentage of survey respondents who said insider threat remediation cost in excess of $100,000

– Tripwire 2017 Insider Threat Report

I put around it and keep wrapping it? It's kind of like an onion," he says. "You want to put layers of controls around [it]. The more layers of controls that I can put around it the better I can maintain that kind of structure."

Mead says each means of control — detection, deterrence, and post-breach forensics — has a varying role to play. "If dealing with an unwitting insider, DLP (data loss protection), coupled with easy-to-use encryption tools, may mitigate the scenario leaving a limited role for IDS (intrusion detection systems) or post-breach forensics," he says. "When looking at the actions of an outsider impersonating an insider, particularly one with privileged IT administrative access, detection and forensics will likely play a very strong role. Understanding the relative risk to a particular organization of each scenario should help dictate the right level of emphasis on each category."

Robert J. Hudock, Epstein Becker Green,

However, defenses need to be tested in threat-driven risk scenarios in order to determine how effective they would be for any one organization's needs, he notes.

"When focused on the unwitting insider, prevention defenses can be very powerful," he says. "From training and awareness to controls that prevent a user from taking the wrong path while simultaneously pointing them to the right one, these approaches can keep those who have good intentions on the right path. Preventative defenses for malicious insiders are more problematic, particularly as many of the insiders in this category are aware of the gaps in prevention and take advantage of them."

Olson believes organizations need to prioritize detection and prevention ahead of post-breach forensics, since these are the controls that provide the most formidable obstacle to those wishing to do the organization harm.

"Many organizations are rapidly becoming better at both of these tasks," Olson explains. "Anti-virus ... is improving, monitoring is becoming more common, as is patch management planning. The net result is that adversary dwell time, the amount of time an attacker has access to a host before they are noticed, is decreasing."

Winning over the C-suite is the necessary precursor to all of this, however. Olson says that if you do not have high-level approval, bolstering data privacy and fighting insider threats simply will not be a priority.

"Having executives establish high-level security and privacy policies is important to setting the tone for the organization, which will translate into data and privacy protecting controls and behaviors being implemented at the lower levels of the organization."

Once you understand the motivations of the company's executives, you can talk to them about the importance of thinking of their data as something that needs to be secured. Some of the most important information in many companies, he notes, takes the form of unstructured data, because those who write it and save it are thinking only of the ideas, and not of protecting them.

Rushing notes, "I can talk to them and say, 'Could you add this meta field into the properties so that we can track it?'" But that works best if they understand what is at stake. ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editor, 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.

316

The average number of days it takes to detect critical web app flaws

– WhiteHat Security 2016 Web Applications Security Statistics Report

Sponsors

ARCTIC WOLF

Arctic Wolf answers the question, “Am I Safe?”, with our turnkey SOC-as-a-service. AWN’s Concierge Security Engineers improve threat detection by up to 10X, leveraging our hybrid AI, custom rules engine and security optimized data architecture. These innovations provide a superior threat detection and response platform for proactively hunting threats, performing remote forensics analysis of incidents, and delivering actionable remediation recommendations.

For more information, visit us at www.arcticwolf.com

FORCEPOINT

Forcepoint is transforming cybersecurity with systems that understand people’s intent as they interact with critical data and IP, enabling companies to empower employees with unobstructed access to confidential data. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide.

Visit www.Forcepoint.com and follow us on Twitter at @ForcepointSec.

wombat™ security
a division of proofpoint.

Wombat Security, a division of Proofpoint, provides information security awareness and training software to help organizations teach their employees secure behavior. Their SaaS cyber-security education solution includes an integrated platform containing broad assessments, a library of simulated attacks and brief interactive training modules, to reduce employee susceptibility to phishing attacks and malware infections up to 90%.

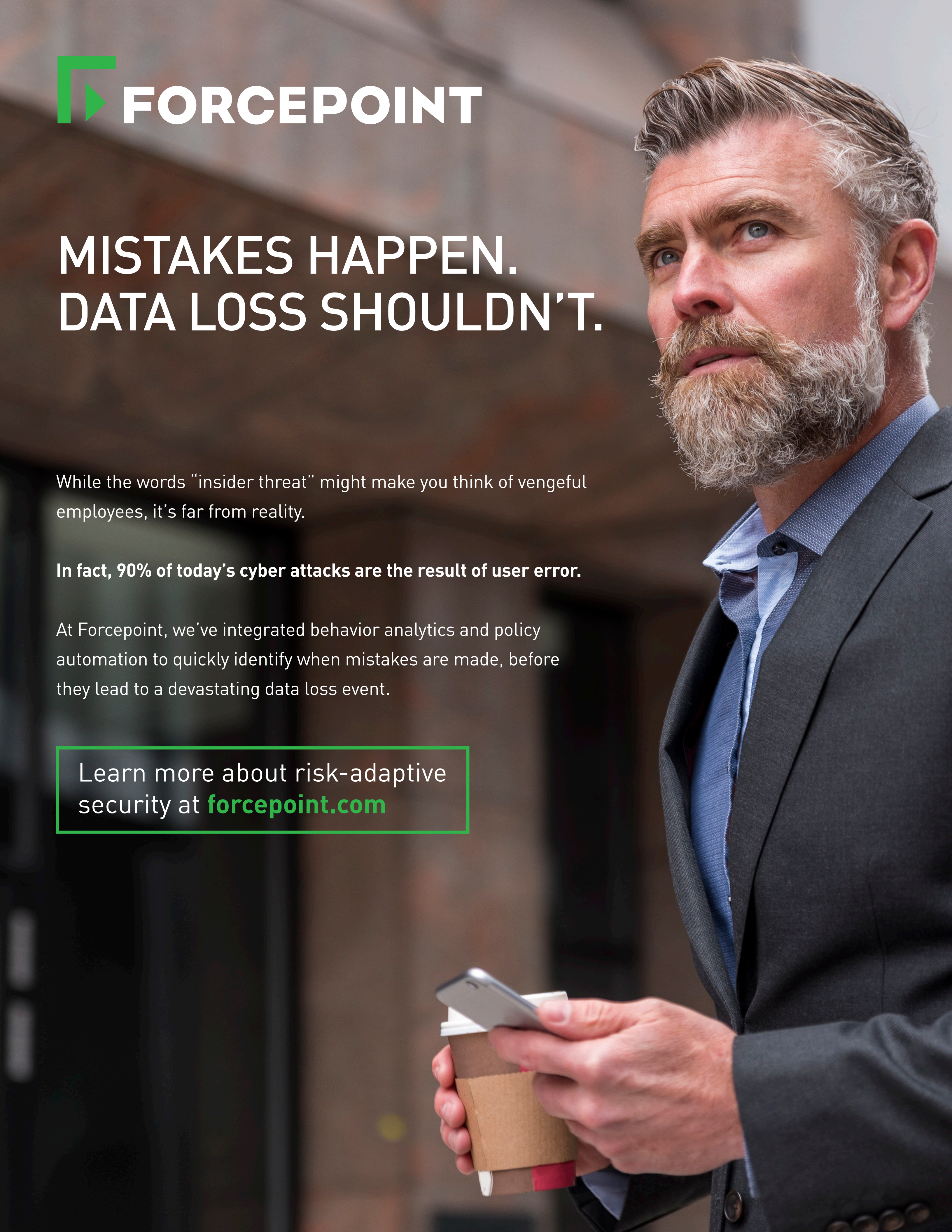
For more information, visit us at www.wombatsecurity.com/modules

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
SPECIAL PROJECTS EDITOR Stephen Lawton
stephen.lawton@haymarketmedia.com
CUSTOM PROJECTS COORDINATOR
Samantha Lubey
samantha.lubey@haymarketmedia.com

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com

SALES
VP, PUBLISHER David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
VP, SALES Matthew Allington
(707) 651-9367 *matthew.allington@haymarketmedia.com*



wombat™ security
a division of proofpoint.

Insider Threats: Are Your End Users Prepared?

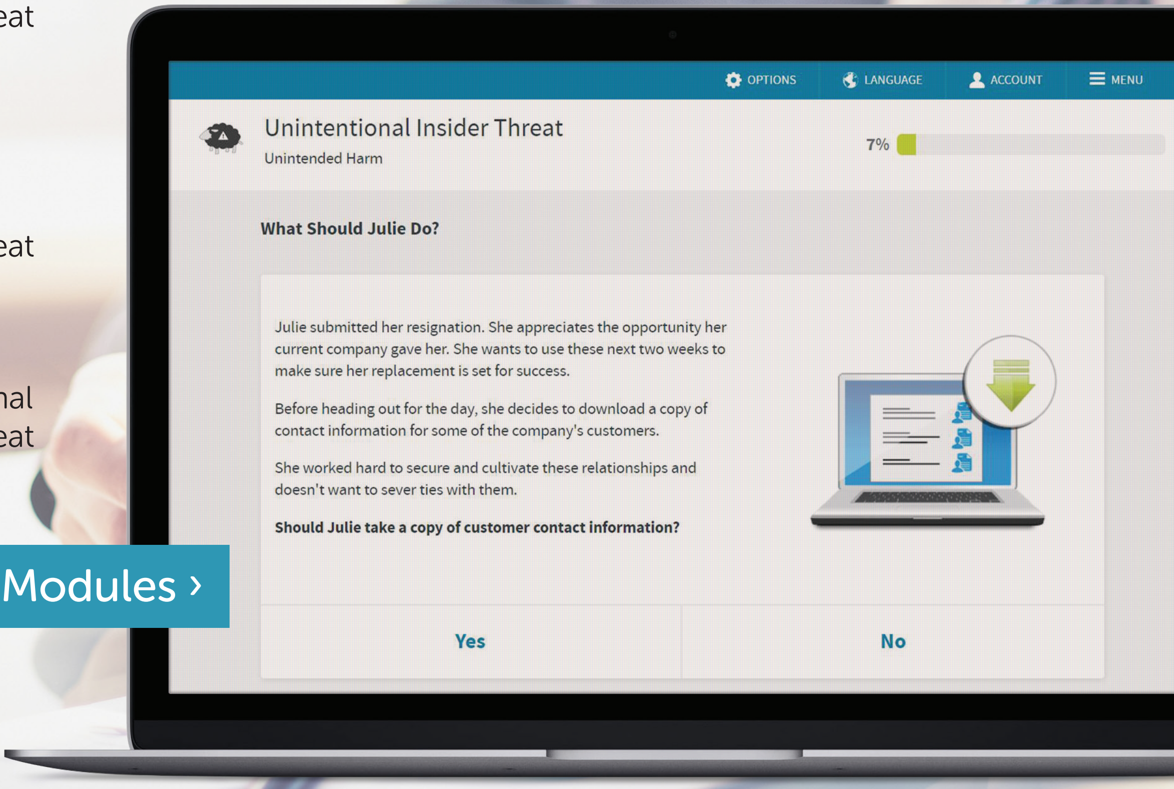
Educate Employees Using Proven Learning Science Principles

Being aware of the threats originating inside your organization is critical. Cybercriminals are seeking to exploit the people inside your company, and current or former employees may misuse access to sensitive information for personal or professional gain.

Wombat Security's new Insider Threat series of interactive training modules will teach employees how to recognize insider threats and basic best practices to protect against them. The modules use real-world examples and scenarios that highlight everyday actions employees take that cause, prevent, or mitigate insider threats.

- Insider Threat Overview
- Malicious Insider Threat
- Unintentional Insider Threat

Try Our Training Modules ›



Unintentional Insider Threat

Unintended Harm

What Should Julie Do?

Julie submitted her resignation. She appreciates the opportunity her current company gave her. She wants to use these next two weeks to make sure her replacement is set for success.

Before heading out for the day, she decides to download a copy of contact information for some of the company's customers.

She worked hard to secure and cultivate these relationships and doesn't want to sever ties with them.

Should Julie take a copy of customer contact information?