Ebook

Forcepoint | Powered by ConversationalGeek

The Complete Guide to Insider Risk

by Derek A. Smith,
September 2020

forcepoint.com

As a former Special Agent for several federal agencies, I have seen firsthand the damage insiders can cause to business and government entities. Your systems are only as good as the people and credentials you trust, and if you cannot trust your own people, then who can you trust? Well, that's the million-dollar question, isn't it, literally? You see, recent high-profile data breaches have shined a spotlight on the risks surrounding these "trusted" employees upon which we rely so heavily and the cost of breaches caused by them.

When it comes to dealing with data breaches and security threats, outside threats tend to get more attention, despite the fact that, according to past experiences, most threats happen because of compromised, inadvertent, and malicious users in your network. It's time businesses stopped primarily focusing attention and resources on external threats and started paying close attention to the internal risks that may be lurking within their networks.

An overwhelming majority of organizations (90%) feel vulnerable to insider attacks, with over half (53%) having experienced insider attacks against their organization in the previous 12 months.[1]

These attacks are only becoming a larger issue to address, as nearly three-quarters (72%) of organizations feel insider attacks have become more frequent,[2] and over half (53%) believe detecting insider attacks has become "significantly to somewhat more challenging" since migrating to the cloud.

This data demonstrates that insider risk continues to increase and that the most significant work that needs to be done is around designing and building effective insider threat programs, including implementing user activity monitoring (UAM)—all of which I will discuss within this book.

Additionally, insider risk can be quite costly; the average annual cost of an Insider Threat rose by 31% in two years to $11.45 million globally, resulting in an average of $4.08 million in losses per year.[3] Most often, negligent insiders were to blame for this monetary loss; employees who make simple mistakes account for 62% of all incidents.[1] It's interesting to note that insider incidents involving credential compromise averaged three times more than those merely involving negligent insiders.[1]

In the investigation world, we have a familiar adage that understanding a criminal's "means, motive, and opportunity" is necessary to prove their guilt in a criminal trial. "Motive" is the reason the person commits the crime, "means" are the tools or methods used to commit the crime, and "opportunity" is the occasion that presents itself to allow the crime to take place. For someone to become a suspect in a criminal investigation, all three must be established. Following this logic, a crime would not have occurred had the perpetrator not had the tools necessary to commit the crime (e.g., viruses, phishing, worms), the actionable idea to commit the crime, and an unencumbered chance to follow through on their nefarious intention.

I want you to keep this theme in mind as I walk you through some critical insider risk considerations, and I am going to add recommended "solutions" for dealing with insider risk.

[1] Cybersecurity Insiders, Insider Threat Report (2018)
[2] Cybersecurity Insiders, Insider Threat Report (2020)
[3] Ponemon, Cost of Insider Threats: Global Report (2020)

What is Insider Risk?

I am sure that anyone reading this book has a pretty good idea of what insider risk is, but I would be remiss in my duties if I did not offer a brief explanation. “Insider risk” is a security threat that originates within a targeted organization.

This doesn’t mean that the threat actor must be a current employee or officer in the organization, or at least appear to be. They could be a consultant, former employee, business partner, board member, or a hacker who has obtained the login credentials of one of these individuals. Internal threat actors are responsible for 30% of all data breaches.[4] Add in the fact that 17% of all sensitive files are accessible to every employee,[5] and you quickly come to realize that insiders have the means (access and privileges), methods (tools), and the opportunity they need to steal your relevant data.

[4] Verizon, Data Breach Investigations Report (2020)
[5] Varonis, Data Risk Report (2019)

Any employee who has insider knowledge and/or access to your businesses' confidential data, IT, or network resources is a potential insider threat. Managing insider risk requires a business to address risks that are in some way or another connected to a trusted identity within the organization (which most risks are, by the way). It's about first determining in detail what employees and other trusted partners are allowed to access within the network and what they can do with the information and resources they access. Then, armed with this knowledge, one can devise a strategy for protecting these identities and company resources.

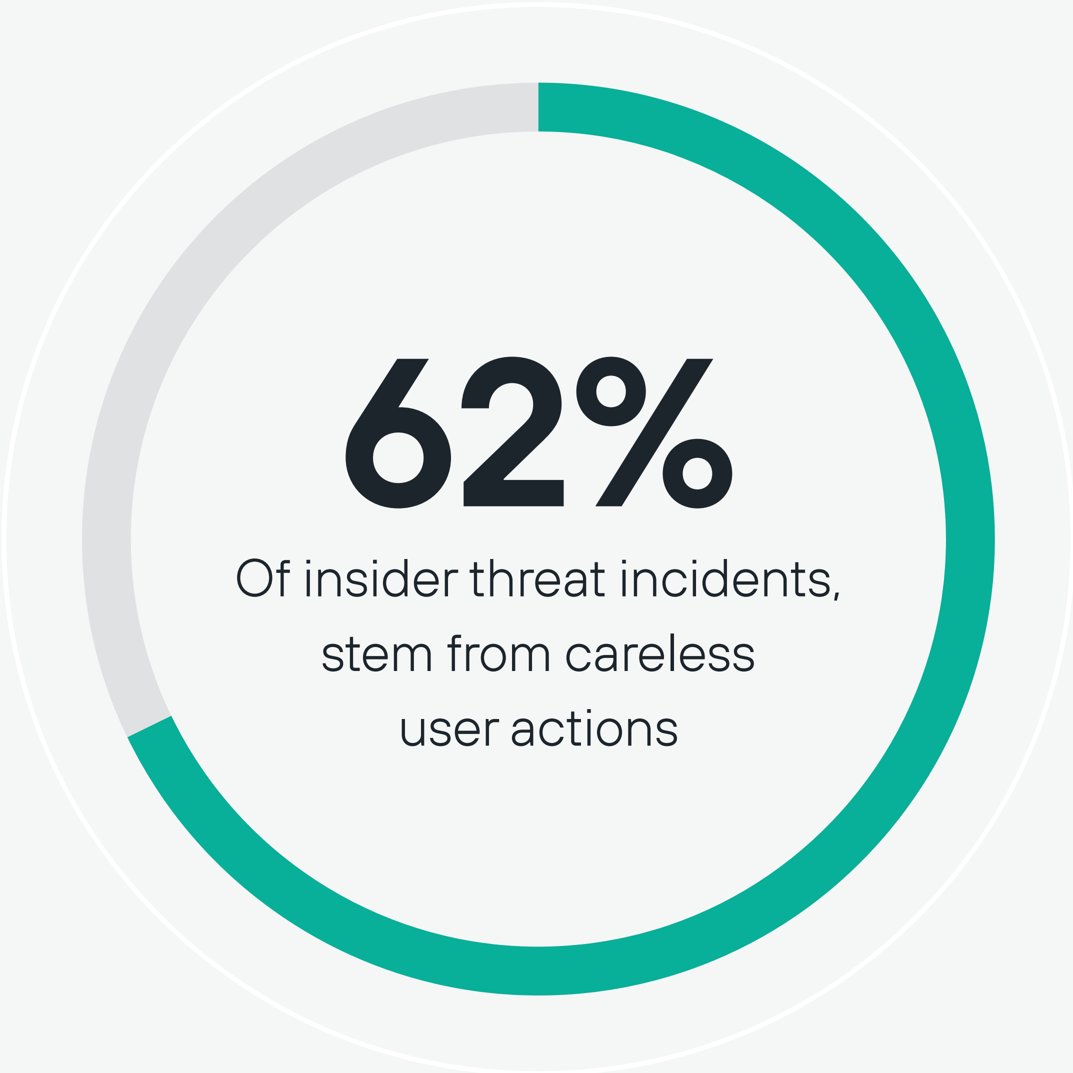
Typically, when I think about insider risk, I think of malicious insiders out for their own gain. But in reality, as I noted before, most insider threat incidents (62%) stem from careless user actions that inadvertently cause security breaches or even as a result of compromised access. Those guilty of exposing critical data are often employees, contractors, and third-party suppliers.

17%

Of all sensitive files are accessible to every employee.[5]

30%

Internal threat actors are responsible for 30% of all data breaches.[4]



Of insider threat incidents, stem from careless user actions

How Can Insider Risks Impact Your Business?

Insider risk prevention is about protection and prevention. An identity thief could get hold of your business information in many ways, and even if you're prudent about guarding your company information, you can still become a victim. Insider incidents cost companies millions each year and can negatively impact your company's cash flow, cause problems with your creditors and suppliers, and even affect your business's reputation.

So, what does this all mean for you and your company? Why is your data in places it shouldn't be? How do you protect yourself against this onslaught? The questions and uncertainty are endless. As a federal agent, I was concerned with a perpetrator's means, motive, and opportunity. These are the keys to solving any crime, and cybercrime is no exception. While all threat actors have motives, insiders have ideal means and opportunity. This places them in a unique and optimal position to carry out damaging activities within your business.

Insider incidents are among the most damaging risks financially. Incidents involving negligent employees or contractors cost an average of $307,111.[3] This more than doubles to $756,760 for insiders who intentionally steal data or conduct other malicious activities.[3] The cost for damage done by external imposters is almost triple at $871,686.[3]

Defensively, it does not matter that data loss stems from an external attacker with stolen credentials or an employee acting carelessly. Your critical data should be protected, no matter who accesses it. The threat is significant because the perpetrators are already inside your network. If you don't protect your data by monitoring the activity and behavior of those that have access to it, you won't be able to respond to any threats they pose, and this can have devastating consequences.

$307,111	Average cost of incidents involving negligent employees or contractors
$756,760	Average cost of incidents involving insiders who conduct malicious activities
$871,686	Average cost of damage done by external imposters

Why Are Insider Risks So Dangerous?

It is not easy to detect insider risk. The insider already has legitimate access to your information and assets, and distinguishing between a user's normal activity and potentially malicious activity is a challenge.

Insiders typically know where you store your sensitive data, and they often have elevated levels of access. On average, it takes organizations more than two months—77 days—to contain insider incidents.[3]

As a result, a data breach caused by an insider is significantly more costly for organizations than one caused by an external attacker; at the time of writing the average annual cost of an insider incident was $8.76 million, while the average cost of a data breach over the same period was $3.86 million.[3]

Insider risk is a significant danger to your organization because insiders have a distinct advantage when working to compromise your systems as they are typically familiar with your data structure and where your intellectual property resides. They may also know how that information is protected, making it easier for them to circumvent any security measures. This insider knowledge makes insider risks harder to defend against than attacks from outsiders since the insider already has legitimate access to your organization's information and assets.

> Because an insider does not need to hack into your network through the outer perimeter—they already have access and are often able to blend in with justified business behaviors.

Another important fact to note is that very few insider incidents are planned and carried out intentionally by a malicious insider. Many incidents are caused by your employees' or trusted partners' negligence. For example, a current employee or contractor might unintentionally exceed their authorized level of access, possibly enabling others to act on their behalf, and consequently harm your organization when a malicious outside (or malicious inside) party perpetrates the final incident. The most frequent categories of insider incidents involved unintentional exposure of sensitive data by a negligent insider and the theft of intellectual property by a malicious insider.

A 2017 report from Haystax titled, "Insider Attacks: 2017 Insider Threat Study," found that privileged users, including managers with access to sensitive information, are the most significant insider risk to their organization. Trusted partners (contractors and consultants) finished a close second, and company employees third. The report discovered clear evidence (investigators love evidence) that insider risk is a growing problem.

Dealing with Insider Risk

The good news is that, despite the difficulties around distinguishing between normal and malicious activity, there are ways to deal with insider risk.

01 **Means**—the tools or methods used to commit the crime

02 **Motives**—Insider Threat Types

03 **Opportunity**—The Occasion That Presents Itself to Allow the Crime to Take Place

Means—the tools or methods used to commit the crime.

Malicious Insider Indicators of Behavior

Now that we know the types of perpetrators we are dealing with, it's time to understand what to look for. As an agent, I focused on looking for crime indicators, and this is no different for compromised or malicious insiders. Watching for anomalous activity at the network level can help identify an inside risk. Similarly, if an employee appears to be dissatisfied or holds a grudge, or if an employee starts to take on more tasks with excessive enthusiasm, this could indicate malicious activity.

Some insider threat indicators you would want to monitor include:

→ Activity at unusual times—signing into the network at 3 am

→ Volume of traffic—transferring too much data via the network

→ Type of activity—accessing unusual resources

Modern Insider Risk Pain Points

Some risks are driven by external events and factors that are outside of your direct control. However, some risks are inspired by internal events and user activities that you can control. Examples include illegal, inappropriate, unauthorized, or unethical behavior and actions by users in your company.

These behaviors include a broad range of internal risks from users:

- → Sensitive data leaks and data spillage
- → Violations of confidentiality
- → Intellectual property (IP) theft
- → Fraud
- → Insider trading
- → Violations of regulatory compliance
- → Conduct risk

Your authorized users have access to create, manage, and share data across a broad spectrum of platforms and services. And if your business operates as most do, you have limited resources and tools to identify and mitigate organization-wide risks while also meeting user privacy standards. The thing is, Insiders can operate in relative silence and potentially inflict more damage than outsiders because they already have a degree of trusted access and direct insight into your organization’s "crown jewels." They conduct movement throughout the enterprise, either on-premise or within the cloud (if you use it).

Motives—Insider Threat Types

To understand the reason people commit insider crimes, we need to understand the insider threat archetypes. These are the people whose behavior exposes your business to data loss and potential damage to your business's reputation.

You can find many descriptions of the different types of insiders behind these threats, but I have selected the basic descriptions defined in the Verizon 2019 Insider Threat Report:

→ **Disgruntled employees**—Many things can make employees dissatisfied: missing a promotion or raise, poor relations with coworkers and managers, etc. These disgruntled insiders can use their position to cause severe damage to your company.

→ **Malicious insiders**—These are employees who misuse or abuse their access to steal, leak, or delete valuable business data out of malicious intentions. Their motivating factors are the main difference between malicious insiders and disgruntled employees. Disgruntled employees abuse data as an emotional response.

→ **Inside agents**—Espionage between nation-states is hardly a new phenomenon, but in the past few decades, nation-states have resorted to a new realm of spying: cyber espionage. These are spies inside your company. An inside agent can be either a newcomer or a trusted employee whose goal is to steal your professional secrets in exchange for a reward from these nation-state sponsors.

→ **Regular employees**—With limited access to sensitive data, employees rarely conduct full-fledged insider attacks. However, they can often leak data or compromise your corporate infrastructure inadvertently, either by mistake or by becoming a victim of phishing.

→ **Third-party providers and contractors**—Due to lack of visibility into third-party provider's operations, you usually have little control over cybersecurity when it comes to dealing with them. While you may audit their security controls as part of your selection process, this still does not guarantee you will be completely safe as you continue to use their services. It is best to have measures in place to protect your remote connections from malicious subcontractors or compromised accounts.

The Reason for Committing Insider Crime

Now that we understand the key players when it comes to insider risk, let's take a look at why they commit the crime. They target company assets for a variety of reasons. Typically, these insiders focus on data that they can easily sell (such as personal information of your clients or employees), or that can be crucial to your company operations (such as your marketing data, financial information, or intellectual property).

Frequent targets of insider attacks include:

→ Databases

→ File servers

→ Endpoints

→ Specific applications

→ Mobile devices

→ Networks

→ Cloud storage

But techy stuff aside, your most important takeaway here is that malicious insiders seek to exfiltrate critical information from your company and your number one mission (if you choose to accept it) is to protect that information.

To get a sense of how insider threats have been perpetrated, here are a few of the most notorious insider threat breaches of the recent past.

1. Anthem: Employee Data Exfiltration

Anthem was hit with an insider theft that resulted in personal data being stolen for over 18,000 Medicare members. In April 2017, Anthem's Medicare insurance coordination services vendor learned of an employee that had been stealing and misusing Medicaid member data since as early as July 2016.

The employee, among other infractions, emailed a file containing data regarding Anthem members to his personal email address. The data included Medicare ID numbers, Social Security numbers, Health Plan ID numbers, names of members, and dates of enrollment.

→ **Lesson Learned:** Just as in a criminal investigation, understanding the where, the how, and who is interacting with your critical data is critical to safeguarding it.

2. Target: Third-Party Credential Theft

Target's highly publicized 2013 credit card data breach is one of my favorites when I speak to groups and students about insider threat. It resulted from a third-party vendor (another type of insider) taking critical systems credentials outside of an appropriate use-case. Access to the credential allowed hackers to take advantage of weaknesses in Target's payment systems to gain access to a customer database and install malware. Additionally, they were able to steal personally identifiable information (PII) of Target's customers, including names, phone numbers, emails, payment card details, credit card verification codes, and more.

→ **Lesson Learned:** This breach serves as a warning that malicious individuals can be creative when it comes to gaining access to your vital systems and data.

3. RSA: Employees get Duped by Phishing Attacks

Sometimes insider threat risk is not malicious but is instead caused by negligence. In the case of RSA, employees clicking on targeted phishing attacks led to a successful advanced persistent attack that may have compromised 40 million employee records.

In March 2011, two hacker groups coordinated with a foreign government to launch phishing attacks at RSA employees, pretending to be trusted coworkers and contacts. When the employees fell for the attacks, the hackers gained access and were able to compromise authentication tokens.

→ **Lesson Learned:** Your most significant assets, your employees, vendors, and contractors, could also be your most significant risk.

4. Sage: Unauthorized Employee Access

Sage is a UK-based accounting and HR software provider that, in 2016, was hit with an insider-caused data breach that compromised 280 of its business customers. A woman who worked for the company used unauthorized access to steal private customer information, including salary and bank account details. While this breach was relatively small in scale, it illustrated the problem of insiders who can gain access, authorized or not, to highly sensitive customer data.

→ **Lesson Learned:** In addition to implementing and enforcing least privilege access policies, businesses must ensure that the appropriate people are alerted immediately when an employee gains unauthorized or unnecessary access to highly sensitive data.

5. Boeing: The Nation-State Spy

During my time as a special agent, I have had to deal with spies. To most people, spies are people you see in TV dramas and films but not in the real world. However, businesses can and do find themselves victims of nation-state sponsored insider threats. One such individual is Greg Chung, who spied for China while working for Boeing, stealing hundreds of boxes of documents about military and spacecraft from 1979 to 2006. No one has any idea the monetary value of all the data Chung stole nor the repercussions of his actions.

→ **Lesson Learned:** Nation-state spying is a reality and an excellent example of risky user behavior that you should have visibility into across all of your systems.

I hope these examples and the lessons learned from them open your mind to the motivations of some of the archetypes and the methods that have been used to attack businesses in the past. This knowledge may help you to prepare for the future.

Opportunity—The Occasion That Presents Itself to Allow the Crime to Take Place

Why are Incidents of Insider Incidents Increasing?

There are many reasons why insider risk incidents are increasing. The growing use of cloud computing technology and bring-your-own-device (BYOD) policies have contributed to a rise in insider threat occurrences. Now, more than ever, especially with the COVID-19 Pandemic, employees are being provided with increased network access. It has been estimated that 56% of the U.S. workforce have compatible jobs (at least partially) with remote work.[6] Currently, only 3.6% of employees works from home half the time or more, with 43% of the workforce working from home at least some of the time. However, the longer people are required to work from home during the pandemic, the more likely they will continue working from home when the dust settles.

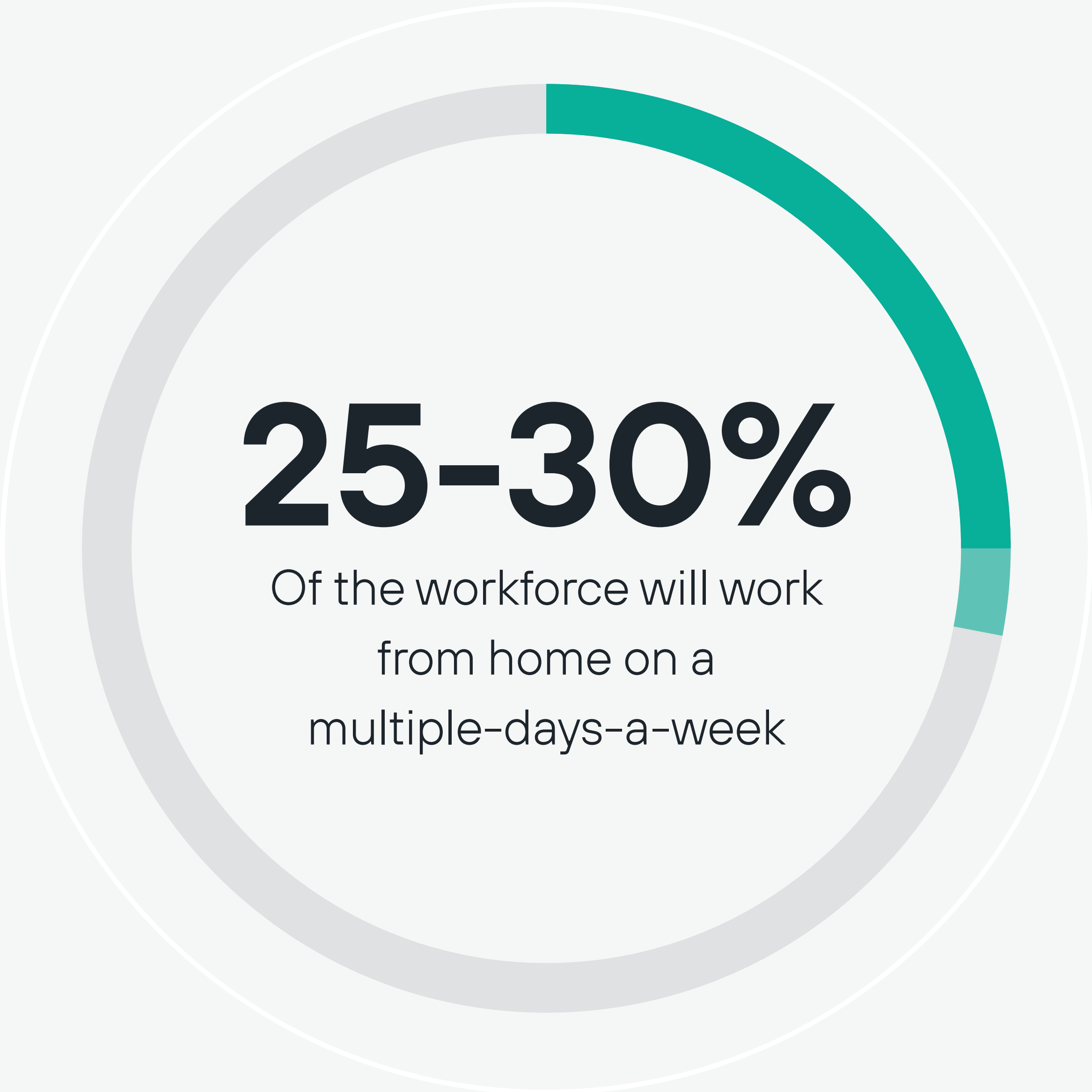
[6] Global Work Place Analytics Work-At-Home After Covid-19 Forecast

Global Workplace Analytics predicts that those who were working remotely before the pandemic will increase their frequency after they are allowed to return to their offices. While for those who were new to remote work until the pandemic, there will be a significant increase in their adoption of working remotely. The company estimates that 25-30% of the workforce will work from home on a multiple-days-a-week basis by the end of 2021.[7]

This sudden and drastic increase in home working has led to a general lack of supervision due to managers trying to keep up with the demand. The consequence is an increased possibility for malicious insiders to go undetected by security systems built to defend against outside threats.

On top of this, there's also the changing nature of work for many organizations with an increasing reliance on contractors and third parties for services, and the fact that attackers and cybercriminals are becoming much better at stealing credentials and brute-forcing their way into corporate networks.

Despite the documented increases in the frequency of these types of breaches, many businesses depend on traditional defense systems that focus solely on preventing attacks through a firewall, anti-virus, or other perimeter solution. This lack of focus on the importance of securing critical data demonstrates the need for a different approach to dealing with insider threats.



[7] Global Work Place Analytics Telecommuting Statistics

What’s the solution?

Generally, as an investigator, my job would be complete once I had conducted my investigation, determined the means, motives, opportunities, and brought the perpetrators to justice. But for the purposes of this book, I need to take things a step further and provide you with some recommended strategies and solutions for combatting insider risk.

Your ability to quickly detect and respond to risky insider behaviors is crucial for the safety and security of your business. Remember, as previously mentioned, it’s taking an average of 77 days to find and contain an insider incident.[3] Understanding why and how insider threats are perpetrated can help you build a comprehensive insider risk program and strategy. You must understand the user behaviors that indicate an attempted data exfiltration or breach and which risk factors are most important to track.

The more visibility you have into user behavior, and the better your alerting system is at identifying signs of an insider threat, the more likely you will be able to catch a malicious insider in action and put a stop to their behavior before the consequences spiral out of control and land you in the headlines.

Mitigating Insider Risks— A Preventative Approach

In ILaw enforcement, when it comes to crime, police and investigators spend most of their time being reactive. We show up after the crime has already taken place. We clean up the mess and try to figure out why the crime occurred, and as they say in the industry, “who done it?” However, in modern crime prevention, we try to take a more proactive approach to attempt to prevent a crime before it occurs. This also applies to cybercrime. To mitigate insider risks, I highly recommend that, like modern investigators, you employ proactive preventative strategies and solutions that can stave off devastating insider attacks before they occur.

Such measures should enable you to detect threats that evade prevention systems quickly and accurately. To start, you have to assume that attackers already operate within your network (i.e., trusted employees and partners), and you, therefore, need early visibility and accelerated response to detect incidents. The ability to understand the context behind insider threat behaviors (i.e., motive) and having strategies that detect their activities, combined with employee-training programs, will help you defend against insider risk and strengthen the controls you use to protect your critical assets.

To start, you have to assume that attackers already operate within your network, and you, therefore, need early visibility and accelerated response to detect incidents.

Developing an Insider Risk Program

Governance

A proactive insider risk program should begin with implementing an effective Insider Governance program that identifies your goals for insider risk management. To accomplish this you need to engage with your key stakeholders and examine compliance requirements driven by regulations such as PCI DSS, SOX, HIPAA, or GDPR.

Here are seven goals to keep in mind for your governance considerations.

→ IAM Lifecycle

→ Linked Accounts

→ Identification of Permissions

→ Compliance-based Reviews—PCI DSS / SOX / HIPAA / GDPR / Other

→ Roles

→ Risk-based Reviews

→ Policies

Let’s start with two prerequisite goals that will set you up for success:

1. IAM Lifecycle

A mature Identity & Access Management (IAM) lifecycle will give you the capability to automate zero-day starts (join), changes (move), and stops (leave) for user account access.

→ New users are onboarded, and their accounts are provisioned with proper permissions for the job role.

→ Users moving to different job responsibilities have appropriate access added and unneeded access removed.

→ Users that are no longer in active status (termination, on leave, retirement, other) have their accounts automatically disabled, or permissions removed as defined by the security policy.

2. Linked Accounts

Linking all secondary and non-user accounts to specific owners will reduce your risk of unaccounted-for access.

→ Administrative accounts should be identified to their specific owner and processed accordingly for lifecycle events.

→ Service accounts must be identified and linked to a specific user/owner.

→ Privileged accounts should be individually owned and linked or governed by a Privileged Access Management (PAM) solution.

→ Off-premises accounts for cloud administration should include the owner, and be individually owned and linked.

3. Identification of Permissions

Effective descriptions for each permission should be used to identify what they are evaluating and make informed decisions.

4. Compliance-based Reviews —PCI DSS / SOX / HIPAA / GDPR / Other

If you're holding sensitive data, you must identify the data and its permissions and specify the level of risk per required compliance, and regular reviews should be conducted.

5. Roles

Roles reduce the burden of the review process and increase accuracy. With roles, your access permissions will be grouped, reviewed, and approved for the specific job duties. Permissions granted that are outside the role are visible for further scrutiny.

6. Risk-based Reviews

Risk-based Reviews are certifications performed on accounts and permissions, posing a certain level of risk to the business. Taking a risk-based approach requires the upfront identification of sensitive data and access and scoring its risk level. During periodic certifications, reviews are performed for the accounts exceeding your pre-determined risk threshold.

7. Policies

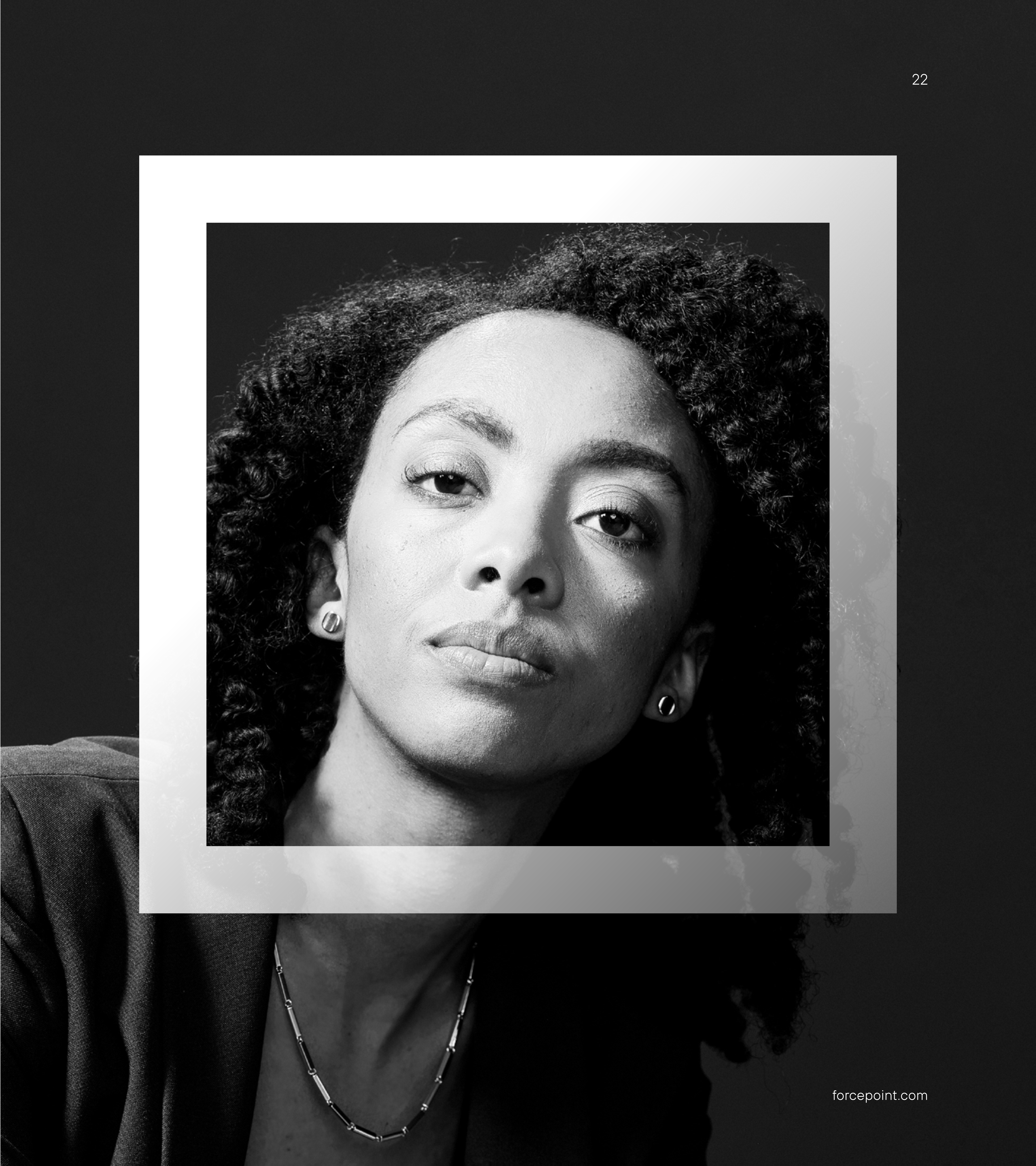
An Insider Risk Governance solution should incorporate the use of policies to identify risk situations (separation of duties or excessive access).

By incorporating these seven goals, you will be able to ensure you're laying the proper foundation for dealing with insider risk.

Creating an Insider Risk Strategy

Once you have created your governance program where you established your insider risk goals, you should determine what your strategy should be for your program.

It's important to remember that dealing with insider risk is a continuous, programmatic process that combines technical and non-technical controls. Your program must incorporate best practices such as personnel background checks, security awareness programs, and policy strategies for social media, BYOD, and IoT devices, among others, with steps that can help your business address insider threats. These are:



1. Determine Which Assets You Need to Protect

You can't protect what you don't know. First, you must pinpoint the areas where problems exist or are likely to occur within your business. This will allow you to prioritize your threats and determine your insider risk tolerance.

→ What are your most valuable information assets?

→ Where are these assets located?

→ Who has access to these assets, and for what purpose?

→ When are these assets being accessed?

→ Are your security controls in line with your risk tolerance?

Answering these questions will provide you with the visibility you need for the critical pieces in your infrastructure that need attention, and what your users are likely to target. You will also know what your normal activity looks like, so you can recognize abnormal patterns of behavior. Additionally, you will also be able to assess your outside partners to determine those who can potentially be an insider risk threat.

2. Continuously Assess Your Security Posture

You must evaluate your organization's security posture continuously. During this evaluation, you should consider threats from insiders and partners, as well as malicious unknowns. Take actions such as:

→ Conduct security program assessments that evaluate your policies, controls, and processes.

→ Initiate an effective threat and vulnerability management program that identifies vulnerabilities that might expose your company to malicious activity.

→ Regularly conduct compromise assessments to determine if malicious insider activity is already taking place on your network.

3. Develop a Formal Insider Threat Program

Next, develop an insider threat program that synchronizes your people, policies, processes, and technology so you can better understand and deter the threats that insiders in your organization pose.

→ Identify internal and external stakeholders, as well as the assets needing protection.

→ Conduct risk assessments to prioritize efforts, focusing on vulnerabilities and threats that target the flow of data in and out of the organization.

→ Involve your security team and stakeholders such as human resources, legal and business groups, along with IT.

→ Consider the lifecycle of an employee, from interview to exit, and determine areas of risk for each step. You should enforce access rules from day one and flag activity outside of access rights.

→ Continuously review privileged access to sensitive information and remove it when deemed unnecessary or high risk.

→ Maintain insider incident-response plans that define response, which should include an extended team (legal, human resources, and departmental management) if an employee is involved.

4. Enforce Separation of Duties and Least Privilege

Two essential controls for reducing the potential for malicious or unintended insider activity are separation of duties and least privilege.

Separation of duties requires that more than one person complete a high-risk task. This reduces the risk of malicious behavior by a single actor.

Least privilege entails restricting use and system access to only the resources required to perform the necessary role or function. This reduces the surface area in which a malicious actor can operate.

These controls should also extend to business partners and contractors.

5. Continuously Monitor User Behavior

Perhaps the most critical step you can take to address insider threats is to learn what's normal behavior and what isn't. The way to accomplish this is by using user activity monitoring and analytics capabilities. There are tools that you may already have deployed within your networks such as DLP, IAM controls, and SIEM. Many SIEMs incorporate user activity monitoring for advanced analytics, user behavior analysis, and cognitive computing-based (i.e., smarter) orchestration and response.

By integrating UAM with IAM, you will be able to proactively remediate some insider threat risk based on real-time user behavior.

Monitoring will enable you to close visibility gaps by aggregating security data into a centralized monitoring solution. Begin with access, authentication, and account change logs then broaden the scope to additional data sources such as a virtual private network (VPN) and endpoint logs as your insider threat use cases mature.

Once the information has been centralized, you may model user behavior and assigned risk scores tied to specific risky events. With enough historical data, you can create a baseline of normal behavior for each user. This baseline indicates the normal operating state of a user or machine so that deviations in this activity can be flagged and investigated. Behavioral anomalies will help you identify when a user has become a malicious insider or if an external attacker has compromised their credentials.

By adopting a user-focused view, you will quickly spot insider threat activity and manage user risk from a centralized location instead of manually piecing disparate data points that individually may not show the full picture.

You will gain visibility into the highest-risk users in your environment and have the proper tools to monitor, report on and investigate them when you develop a detailed understanding of your assets and security posture, a clear separation of duties, continuous monitoring, and a cross-organizational insider threat program. This will help you transform user data into an asset and prevent your organization from making the wrong kind of headlines.

Automate Your Insider Risk Processes

Finally, I highly recommend that to make your insider threat detection process effective, you use a dedicated automated platform that helps you identify malicious intent and mitigate threats.

Some tools you can use for insider risk management include:

→ Identity and access management—to verify the identity of a person trying to access your protected assets.

→ User activity monitoring—to thoroughly monitor and record for threat detection. Your system should be able to power a complete view of when users are trending towards risk by providing context and intent around user behaviors. Additionally, this will allow you to stack rank users by risk to focus your investigative resources strategically.

→ User and entity behavior analytics—to profile your users and predict insider threats based on their behavior. A machine learning algorithm collects patterns of normal user operations, establishes a baseline, and alerts on insider threat behavioral indicators.

→ Alerting and responding capabilities—to create a rules-based alerting system using monitoring data. When a rule is broken, you can investigate the suspicious session, preferably in real-time, so you can manually block users if necessary.

The Big Takeaways

Insider risk detection is challenging, and every company is vulnerable. When an insider attack eventually happens, effective detection, a quick response, and a thorough investigation can save you a ton of money in remediation costs and reputational damage. Therefore, advanced preparation is always best.

For insider risk detection to work, you need to know about potential behavioral signs or indicators, as we investigators call them, that will point you in the direction of a potential perpetrator.

You can manage many aspects of your insider risk program by investing in tools and services that monitor and control users for their own benefit and for the benefit of your company.

Best Practices for Protecting Against Insider Attacks

As a recap, these steps can help you reduce the risk of insider threats:

→ **Get executive buy-in**
Getting the board behind information security policies is much more complicated than it should be, despite all the press given to cybersecurity incidents, but it is essential you have it. Convincing senior stakeholders that engaging and buying into a preventative information security maintenance strategy should be one of your first priorities. You must convince them that this will not only help to mitigate your insider risk concerns, but will also put your company in a better position to comply with the requirements of many more regulatory bodies, as well as making you a much less attractive insider risk target.

→ **Protect your critical assets**
Locate and define your most important assets both physical or logical, this includes systems, technology, facilities, and people. Remember that intellectual property, customer data for vendors, proprietary software, schematics, and internal manufacturing processes are also critical assets.

→ **Enforce policies**
Build a governance policy that you will use to clearly document organizational policies, so you can enforce them and prevent misunderstandings. These policies can be automated by using software that will provide you with the ability to define a security policy, ranging from profiles, to file shares, object-level security settings, object ownership, authorization lists, public and private authorities, and any other controls you need for insider risk reduction.

→ **Increase visibility and focus monitoring on your riskiest users**
To do this you will need to deploy automated solutions to keep track of employee actions and correlate information from multiple data sources.

→ **Promote culture changes**
Ensure the whole company understands that security is not only about know-how, but also about attitudes and beliefs. To combat insider risk, educate your employees regarding security issues and work to improve employee satisfaction.

Forcepoint

forcepoint.com/contact

About the Author

Derek A. Smith has more than 30 years' experience in the security industry. He is a former government agent, cybersecurity SME, and holds a variety of certifications (CISSP, CEH, CCISO, Security+, etc.) as well as eight college degrees. Derek is also a published author, conference speaker, cybersecurity analyst for several international and local television news stations, and a government program manager.

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

The Complete Guide to Insider Risk ebook 28SEPT2020