SUMMER 2020

THE RED BOOK OF INSIDER THREATS

15 Security Leaders Share Their 2020 Concerns & Best Practices

PRESENTED BY DASERA

REAL-WORLD ADVICE ON TACKLING INSIDER THREATS BY THOSE WHO ARE LEADING THE CHARGE

CONTENTS

FEATURED SECURITY EXECUTIVES

Causes of Insider Threats

Pages

10-12

Mark Weatherford
Chief Strategy Officer & Board Member
National Cybersecurity Center

Ankur Shah
VP of Products, Cloud Security
Palo Alto Networks

Julie Tsai
Head of InfoSec
Roblox

Anand Ramanathan
VP of Products & Marketing Enterprise
McAfee

Jitendra Joshi
Head of Information Security
BetterUp

Sujeet Bambawale
CISO
7-Eleven

Rise of Insider Threats

Pages

16-18

Cost of Insider Threats

Pages

22-24

Amol Kulkarni
CPO
Crowdstrike

Christopher Donewald
Privacy Counsel
Affirm

Andy Kim
CISO
AllState

FEATURED SECURITY EXECUTIVES

Detection & Remediation

Pages

21-31

Sameer Khera

CIO
Norton LifeLock

John Hluboky

Principal Security Architect
AllScripts

Hemanta Swain

VP & CISO
TiVo

Marc Ariano

Head of Cybersecurity
Vroom

Siddharth Bohra

Chief Business Officer
Larsen & Toubro Infotech

Shaq Khan

CEO
Fortifire

Ecosystem Speaks

Pages

33-34

Introduction

Insider threats are not new, so what's changed about it in the 2020s? That's what we wanted to answer through this book. Written by some of the leading security and product executives, the **Red Book of Insider Threats** is a biannual publication which will bring you the latest and greatest in this space.

In the Summer 2020 edition, we feature 15 great leaders.

Some of the ideas and thought processes they share in the following pages will help define how you deal with insider threats. Many security professionals we spoke with are in the process of defining a formal insider threat program for their business. Included with the Red Book is a free "Insider Threats Checklist" that will help you assess your readiness to deal with these risks.

Ani Chaudhuri
Cofounder & CEO, Dasera

Ani Chaudhuri

01

CAUSES OF INSIDER THREATS

Where do insider threats arise from? How exactly does one define who's inside and who's outside?

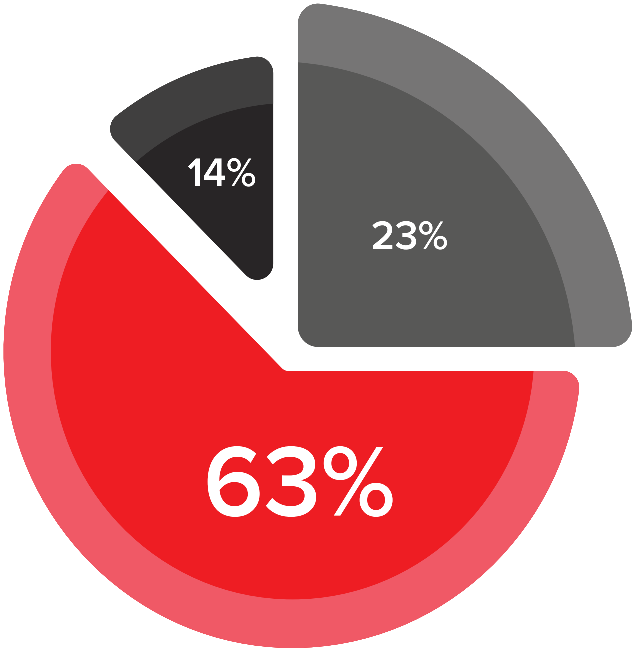
CAUSES OF INSIDER THREATS

The primary causes of insider threats are well known – employees, contractors, partners. In short, anyone who has access to your sensitive data or company networks is an insider. Even if you give temporary access to a third party like a vendor or consultants, they become insiders too. In some cases, companies also consider ex-employees or recently churned employees as insiders.

Several industry reports also suggest that a malicious outsider, who steals the credentials of an insider, should also be considered as an insider.

This raises the question – when does an external attack convert into an "insider" threat? And what insider threat defenses do you deploy when the attacker has already gained access?

So, to get started, do you have a list of your insiders? Without an exhaustive definition for insiders, it is going to be impossible to build an effective defense against insider threats and breaches.



Frequency of 4,716 incidents for three insider profiles

● Credential Thief (Imposter Risk)

● Criminal & Malicious Insider

● Employee or Contractor Negligence

Source: 2020 Cost of Insider Threats Global Report – Ponemon Institute Sponsored by ObserveIT & IBM

INSIDER THREATS
THE UNUSUAL SUSPECTS

Insiders needn't only mean your employees. A truly robust insider threat program will account for many edge cases or scenarios.

THE SNEAKY EX-EMPLOYEE

Employees who are in their notice period or have just left need some extra attention. They may potentially use their credentials to copy files to personal drives, delete or exfiltrate sensitive data in case they left on poor terms.

THE CARELESS CONTRACTOR

Contractors can have long-term or temporary access to company networks or databases. In such situations, the contractors' employees need to be considered as much an insider as those on your own payroll.

THE EVIL CREDENTIAL THIEF

Most data breaches take months to detect. So if a malicious outsider steals employee credentials, they are likely to have access to your network for a long time. We need to understand their intent differently than an inside agent.

THE DISGRUNTLED EMPLOYEE

There are many situations that can cause an employee to be upset with peers, managers, or the company. They can potentially act out in different ways too e.g. just deleting data instead of stealing or misusing it.

Employees present one of the highest cybersecurity risks for organizations. In most cases, employees are not technically adept to understand when they are being careless or are phished by a malicious outsider. This makes insider threats challenging and complex.

Consumer information collected and sold by companies is incredibly profitable for marketing and advertising. And there are many, many players scraping, sniffing, tracking, and gathering personal information from the Internet. Most states have passed some form of privacy legislation (CCPA being a frontrunner among them).

As a result, controls over managing data use has become business critical. I think that most of us will concede that having more control over our personal information is a good thing. We have to adapt internally to ensure we – our tech and our employees - are ready for this future.

BEST PRACTICE SUGGESTIONS

01 Prepare now to navigate through a complicated mix of federal, state, and industry regulations and laws when dealing with consumer data. Ensure none of your own employees act in violation of these laws.

02 A large portion of your supply chain – suppliers, contractors, partners – are also insiders. They can result in as many as 50% of your insider incidents. Develop a program that incorporates your supply chain as well.

03 Establish enterprise-level governance and control policies. Clearly document these policies and ensure that you consistently enforce these rules.

FEATURED EXECUTIVE

Mark Weatherford

Chief Strategy Officer and Board Member
National Cybersecurity Center

> “ Prepare now to navigate through a complicated mix of federal, state, and industry regulations and laws when dealing with consumer data.

FEATURED EXECUTIVE

Ankur Shah

VP of Products (Cloud Security)
Palo Alto Networks

> “Education and training will go a long way in changing the conversation around insider threats.

Back in the days, procurement of IT tools was centralized and owned largely by the IT teams. This allowed enterprises to implement tighter IT and security controls and implement and establish access controls on an “as-needed” basis. Over the last decade, cloud has enabled decentralization of the procurement and management of most (if not all) IT tools. Employees within the business units who are now empowered to manage and configure various cloud services lack common understanding of how to implement security and access controls. As a result, we are going to continue to see a rise in insider threats until proper education, training, and tools have been put in place to stop users from shooting themselves in the foot.

Unfortunately, insider breaches are usually kept under the covers for the fear of enterprises looking silly for leaving gaping holes in their environment. Most of the security industry is focused on technologies for external threats. This is because it’s much easier for these companies to talk about a malicious outsider than innocent insiders. And this is what needs urgent change.

BEST PRACTICE SUGGESTIONS

01 Education and training will go a long way in changing the conversation around insider threats. Companies must implement company-wide education and training programs.

02 Two important technologies that can help: least privileged access controls across cloud services and data protection (encryption and others) for sensitive data.

03 Maintain complete audit trail of who’s accessing what. Also, use behavior analytics to detect normal and abnormal behavior by the insiders.

Insider threats are becoming more important, but also more complex. They are not as simple as one event, one compromised system, or one malicious person. Instead, insider threats can be traced back to a chain of events that leverage multiple vulnerabilities. This makes a company's digital footprint more challenging to manage. It also makes it tougher for security teams to predict how multiple incidents might potentially impact each other. Any new security executive should leverage their existing knowledge (such as attack surface, monitoring levels, staffing proficiency) as well as the specific factors of the business (such as the nature of data, how it is used, whether data users are aware of risks, the contractor/consultant/third party vulnerabilities, etc.).

It is important for security leaders to consider not just the technical risks, but also focus on modeling and communicating the business risks, especially from a continuity and brand reputation perspective. As an example, what is the dollar value of taking down a service in order to ensure it is secure, or vice versa how long can you afford to keep up a service knowing it's not secure. Also, the repetitional impact that a company may have from such a potential incident can be complex to model and predict – especially in a world where loss of personal data can result in many long term and irrational fears about using the company's products or services.

BEST PRACTICE SUGGESTIONS

01 Create a 360-view on insider exploitability – identify data interactions that create least astonishment, the lifecycle and travel path of the data, access privileges, etc.

02 During an incident, taking down a particular asset or service only solves for the incident itself. We need to 'inoculate the herd' in order to prevent recurrence. Track the vulnerability upstream so that remediation isn't focused only on one area e.g. the endpoint.

03 We can't protect what we don't know. Flag & correlate for simple indicators of what shouldn't be happening.

FEATURED EXECUTIVE

Julie Tsai

Head of InfoSec
Roblox

> “We can't protect what we don't know. Flag & correlate for simple indicators of what shouldn't be happening.

02

RISE OF INSIDER THREATS

Why are there more insider threats today than just a few years ago? How are our insiders changing?

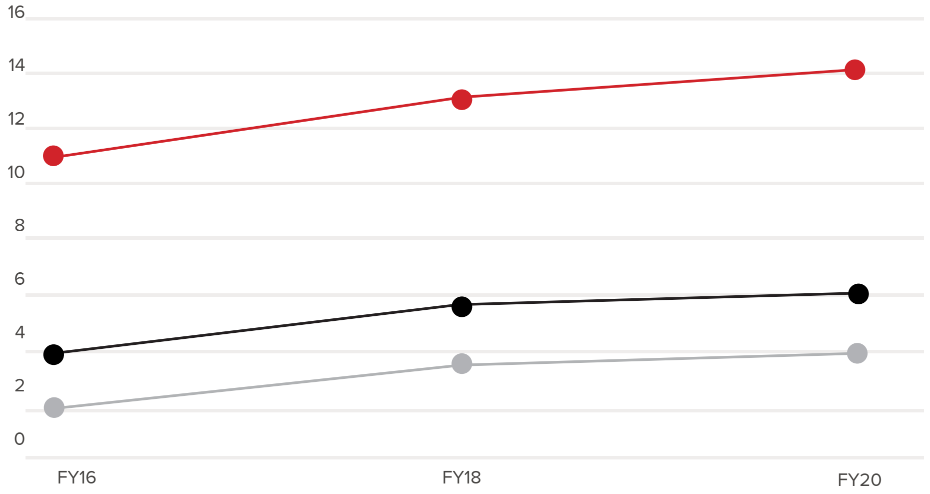
INSIDER THREATS ARE INCREASING

Industry reports suggest that the average number of incidents involving insiders has steadily increased over the last 4 years. Insider threats of all kinds have increased, irrespective of what they stem from – negligence, malintent, or credential theft. The steady increase can be attributed to increased vulnerabilities, greater transparency or federal regulations, or simply to an erosion of human values.

Sixty percent of organizations, one report suggests, had more than 30 insider-driven incidents per year.

As more of our data and applications run on cloud software and teams become globally distributed and remote, these incidents will become more frequent.

On any given day, security teams perceive insider threats as significantly less dangerous compared to external hackers. However, the days of relying merely on training and trust to deal with insiders are far gone. In our research for this book, all the CISOs and security executives that were interviewed said insider threats were going to become more critical and top of mind for them in this new decade.



All Types of Insider Threats Are Steadily Increasing

- ● Employee or Contractor Negligence
- ● Criminal & Malicious Insider
- ● Credential Thief (Imposter Risk)

Source: 2020 Cost of Insider Threats Global Report – Ponemon Institute Sponsored by ObserveIT & IBM

INSIDER THREATS
LET'S PAINT A PICTURE

These are employees you hired for a reason - partners that you trust to run your business. And they are trustworthy, for the most part. But humans are human. We make mistakes. We can be careless. Sometimes, we will let curiosity get the better of us. In our worst moments, we can also be petty, greedy and even vindictive. When insiders handle data, insider breaches are likely to happen. Since insiders are human and insiders are everywhere, insider breaches are everywhere as well.

Britney Spears just checked into your hospital. Tom got to know of it from a friend in another department. He looks up the details on the patient records database and leaked the news to a tabloid for a quick buck.

Lauren's new on the job and wanted to impress her boss with her analytical skills. She downloaded thousands of customers' PII on her laptop to build the report. And then lost the laptop in a coffee shop.

Jason works for a retail company. He is upset over a breakup. He wonders if his ex is already over him and is dating other people. He decides to check her recent purchases to determine how her lifestyle has changed.

For too long, IT security has been seen as the inhibitor of productivity and innovation. In this new decade, IT security teams will start looking at insider threats more intensely while still being conscious of "getting in the way". It's going to be a hard line to maintain, but both aspects are equally critical. Only the CISO and their team can balance these two factors effectively.

External adversaries will constantly evolve their tactics to get around security products, so security teams need to keep innovating and disrupting. The most vulnerable part of the security ecosystem will continue to be the internal humans – employees, contractors, partners – whose mistakes or malicious intent will cause the biggest problems. Internal vulnerabilities can expose businesses to malicious outsiders, so insider threats can quickly become external threats as well. In the 2020s, we will have to think more aggressively about how insiders behave and interact with company assets like customer data.

BEST PRACTICE SUGGESTIONS

01 Reprioritize threat information to ensure you're seeing relevant insider threat metrics as well. These metrics should reflect insider threats that pose a risk to businesses at large.

02 Having an insider threat program can be a great start, but you need complete executive backing for it to be successfully implemented.

03 Structured databases in the cloud can host millions of consumer/customer records in a single machine and pose significant risk from the point of view of mass-privacy violations and million-dollar fines. Given the higher stakes, businesses have to invest more in proactively monitoring access and use of sensitive data.

FEATURED EXECUTIVE

Anand Ramanathan

VP of Products and Marketing (Enterprise)
McAfee

> "Reprioritize threat information to ensure you're seeing relevant insider threat metrics as well.

FEATURED EXECUTIVE

Jitendra Joshi

Head of Information Security
BetterUp

> Build a culture of trust and democratize security which means make it everyone's responsibility...

Our definition of insiders has undergone a massive change. In the post-COVID world, our perimeters have disappeared and the line between trusted insiders and outsiders have blurred. There is no dialing back from here. Companies have to ramp up their security operations to ensure people can work from any machine and network. Insiders cannot be defined by just location, device, or network anymore. We need to enrich the definition of an insider.

Add to that the "matter of trust". Every leader wants to trust, even at companies that have lived through a breach. How you translate your culture of trust to the digital and policy side defines how secure you are. We need to demonstrate to insiders that we trust and value them and giving them the freedom to do what they need to do. At the same time, we need to put in place enough controls to detect anomalies. This decade will be all about policy-driven trust, baseline-driven monitoring and real-time remediation.

BEST PRACTICE SUGGESTIONS

01 Build a culture of trust and democratize security which means make it everyone's responsibility to ensure the safety of the business's crown jewels – consumer data. Also, train people continuously so they understand their role and they feel they are adding value to the process.

02 Establish baselines for secure access, usage, behaviors, etc. Create these benchmarks not just for config, but also for how apps, data, and processes are supposed to function. Then, identify the deviations based on these baselines.

03 In the situation of an incident, act rapidly. As a leader, empower your team to act fast. Do not slow them down with too many protocols to be followed (as is the case in many large organizations). You want remedial action to be swift and effective, not slow and burdensome.

Most of the incentives that drive external threat actors are also valid for insider – compensation, affirmation, or conviction. In the information security space, we believe that "a chain is only as secure as its weakest link". Bad actors might have a greater chance of success by incentivizing internal users towards malicious outcomes rather than mounting system-wide attacks on industry-standard security safeguards.

The security industry, in terms of tools and techniques, has a tremendously deep tranche of innovation and engineering that allows for rapid growth. Enhancements that permit an increase in the depth and breadth of visibility, intelligence, and Prevention – at scale – are evident from both the offerings of young companies and the evolving feature set of existing players. Thus, bad actors may choose to attempt a different tact by doubling down on the human approach. This could manifest in different ways by making it easier for insiders to accidentally misroute confidential information and/or incentivize insiders to part with privileged data and/or privileged access.

BEST PRACTICE SUGGESTIONS

01 We hear "Zero Trust" a lot nowadays, and I like to explain that by summarizing it as "Validate, then Trust" approach to all privilege and resource allocation. This approach can be leveraged to manage the insider threat by validating all working assumptions at every engagement and by actively managing trust.

02 Trust should not persist or be transitive. An entity, programmatic, or human, must not retain the privilege to initiate a trusted action beyond the perimeter of the request that provisioned it. It must also not be able to relay, in part or whole, its privilege to initiate a trusted action.

03 Trust is atomic. Privileges to perform a trusted action are granted to the minimally viable constituent of the system that will dispose that action.

FEATURED EXECUTIVE

Sujeet Bambawale

CISO
7-Eleven

> "Trust is atomic. Privileges to perform a trusted action are granted to the minimally viable constituent of the system that will dispose that action.

03

COST OF INSIDER THREATS

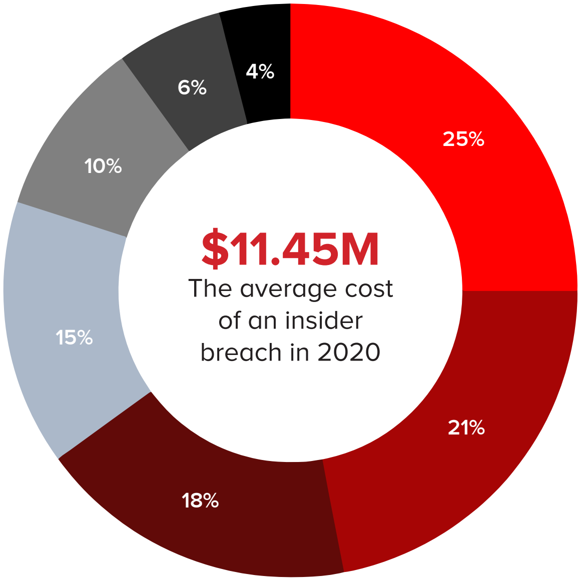
How much does it cost a business to recover from an insider-driven data breach?

COST OF INSIDER THREATS IS INCREASING

The cost of insider breaches is increasing. As per the 2020 Ponemon Report, the average breach today costs 1.4 times what it used to in 2018 and almost 3 times the cost in 2016. The increase in frequency and costs is a double whammy for any security team.

Look at how this cost breaks down. Apart from technology (which has long-term detection and remediation benefits), almost all other cost categories, amounting for 79% of the cost, are disruptive in nature – they upset our well-laid business plans and hurt business continuity.

This cost does not include the opportunity cost of lost business. In today's day and age, breaches receive significant media exposure and result in a strong erosion of consumer trust. When your brand reputation suffers, it is tough to estimate how it impacts your growth as a business.

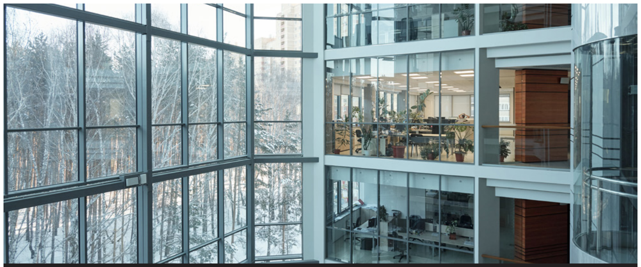


Percentage Cost of Insider Incidents by Standard Categories (N=204)

Source: 2020 Cost of Insider Threats Global Report – Ponemon Institute
Sponsored by ObserveIT & IBM

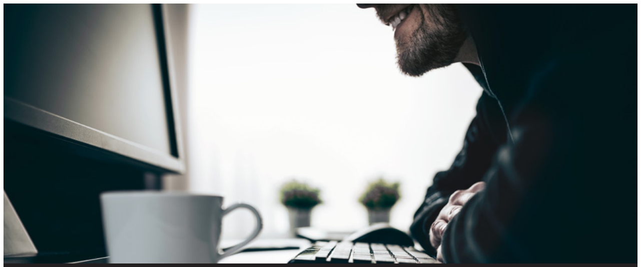
COSTS VARY BASED ON MANY FACTORS

$11.5M is a lot of money. For an early, venture-backed startup, it may mean an existential threat. In many cases, we also see courts and regulatory authorities consider the company's revenue and size in determining the value of the settlement or fines. Here are some factors that impact the average cost of your breaches.



BIGGER COMPANIES PAY MORE

For companies that have more than 25,000 employees, the average cost of a breach jumps from $11M to $17-18M. For companies smaller than 5,000 employees, the same number is in the range of $7-8M. Bigger companies also have more insiders who have access to sensitive data, which increases their exposure to risk.



CREDENTIAL THEFT COSTS MORE BUT IS LESS FREQUENT

The average credential theft costs almost 1.8 times more than the average negligent insider. However, businesses have traditionally trained their security focus on the 'evil outsider' and relied on trust and training to deal with insiders. As a result, businesses face many more insider-related breaches. This makes the annualized cost of insider breaches almost 3 times more than those caused by credential thieves.

Companies have been aware of and working on insider threats for a while now. However with accelerated digital transformation across industries, insider threats are now also becoming as complex and distributed as a potential cyber attack. CISOs can no longer afford to view slices of threat data across systems and workloads. We have to digitally correlate what's happening across the entire spectrum of assets e.g. data stores like S3, individual endpoints like employee laptops, networks, and connections.

The recent COVID situation has further accelerated the need for expanding the scope of our insider threat monitoring and remediation capabilities. Our systems have seen a 330% increase in e-crime attacks since companies adopted remote work, many of which can leverage an insider or an insider's credentials. The attack surface has grown, making our networks vulnerable. As a result, perimeters and perimeter-based security will take a backseat compared to action-based frameworks, anomalous behavior detection, and true zero trust approaches.

BEST PRACTICE SUGGESTIONS

01 Create 100% coverage from a monitoring perspective. Companies must possess deep visibility end to end across assets and workloads. Another area to focus on is linking the runtime visibility with changes to configuration being made in near real-time.

02 Build prevention capabilities like blocking an exfiltration attempt, flagging or unflagging identified anomalies, restoring backups, and estimating the impact radius of an incident.

03 We must build monitoring and remediation capabilities that add no friction to the teams that leverage data and files for their work. That would mean security at DevOps velocity where you provide observability without reviews or approval hoops for people to jump through.

FEATURED EXECUTIVE

Amol Kulkarni

Chief Product Officer
Crowdstrike

> “We must build monitoring and remediation capabilities that add no friction to the teams that leverage data and files for their work.

FEATURED EXECUTIVE

Chris Donewald

Privacy Counsel
Affirm

> “Know Your Data: every company needs to know its data asset inventory down to the last data field.

Insiders are particularly dangerous because, unlike black hats working to penetrate a company’s system, an insider typically has legitimate access to the system. Insider threats can result from careless employee behavior such as an oversimplified password or clicking on links they should know not to touch. As IoT, data use, and regulatory frameworks become more complex across the globe, companies who lack the necessary understanding, training, and education will face the inevitable insider breach.

Companies should perform regular company-wide risk assessments in order to understand the risks it faces with the processing of data (i.e., avoid not knowing what you don’t know). Companies should implement, enforce, and, perhaps most importantly, regularly update policies and controls to account for routine uses of data and any new uses of data. Further, it is crucial that a company maintain a healthy incident response plan built around speed and maximum communication to mitigate fallout from an insider breach. Not only will this minimize harm to consumers, but it will also save the company significant financial and personnel-time cost.

BEST PRACTICE SUGGESTIONS

01 Know Your Data: every company needs to know its data asset inventory down to the last data field.

02 Sensible Access Controls: if an employee does not need to process a particular data field to perform his or her role, that employee should have zero access to that data. To permit otherwise risks the start of a chain reaction leading to an insider breach.

03 Thorough and Regular Training: As data use becomes more complex, employees must understand what processes are permitted and which are not. Data stewardship begins with the organization.

FEATURED EXECUTIVE

One of the most challenging aspects of a business today is the risk of a loyal employee going rogue. In many circumstances, insider threat isn't a risk that is immediately recognized and occurs almost imperceptibly over time. To add additional complexity, insider threats as a threat itself is difficult for management to recognize unless there is a laser-like focus on how the business operates with its customers, employees, and vendors in the context of fraud.

Insider risk impacts every organization big or small. Understanding insider risk involves a close evaluation of how your business operates with your customers, employees, and vendors. Knowing the customer journey, recognizing the complexity of human motivation, and identifying incompatible job duties is an initial jump start to combat insider risk. The journey, however, does not end there. Insider risk is an ongoing program that needs continuous monitoring and evaluation to be effective.

BEST PRACTICE SUGGESTIONS

01 Understand the Customer Journey – At Allstate E-business, we are in the business of selling insurance online. We closely track false internet identities who collaborate with rogue employees to game the online insurance purchase process for financial gain or to cover products that would not normally qualify.

02 Understand Staff Temptations – People are highly complex in terms of what motivates them, e.g. someone with financial problems may think they are entitled to a share of company profits. Such employees in Customer Account Setup, Treasury, Accounting, or HR can do serious financial damage.

03 Understand Incompatible Duties – Long-term staff have deep institutional knowledge, which makes them powerful but also puts them under high risk. Employees who care about the business will tell you, I could do that, but I don't think I should. But in the vast majorities of situations, this presents an opportunity for insider risk.

Andy Kim

CISO
AllState Insurance

> “Understand incompatible duties - Long-term staff have deep institutional knowledge, which makes them powerful but also puts them under high risk.

04

DETECTION & REMEDIATION

How do business monitor potential risks? And how do they proactively save themselves from breaches?

METHODS OF THREAT PREVENTION

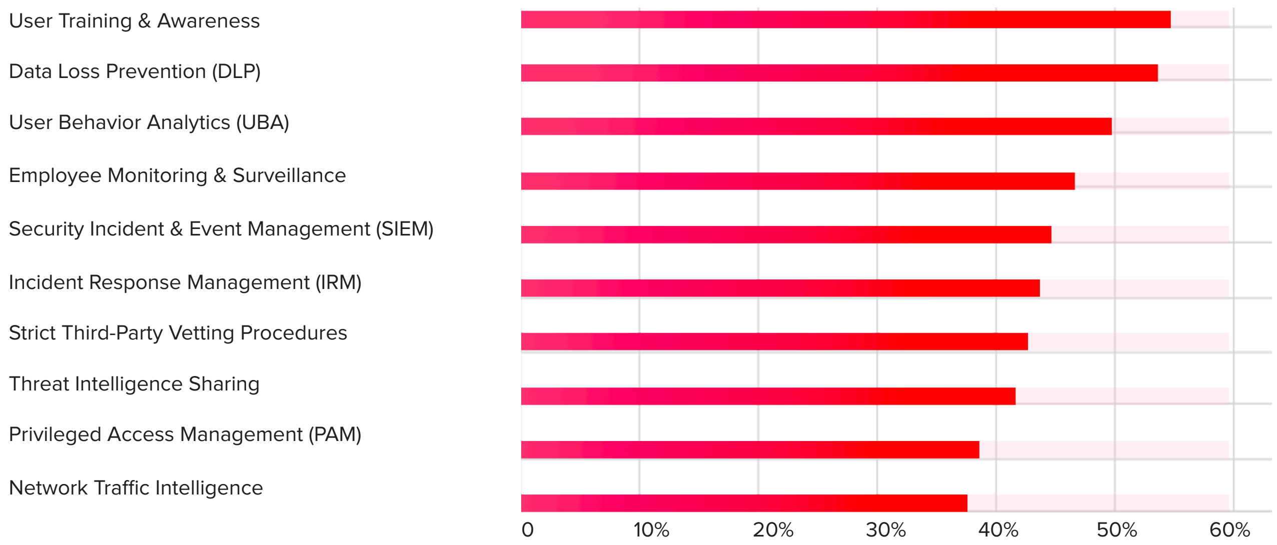
The most used method to prevent insider threats continues to be user training and awareness with 55% companies saying they use these methods. And yet, if you read articles on the top breaches this year, every one of them was either directly or indirectly perpetrated by a negligent, careless or malicious insider.

Companies are clearly waking up to the fact that training and trust cannot be the primary prevention method when dealing with humans. Humans, after all, are prone to making mistakes.

Lapses in judgement happen all the time. As a result, companies have increased their investment in technologies like DLP and UBA systems that help them prevent data from leaving the premise or understand employee behaviors better.

Leveraging data is now a key competitive differentiator. This means giving more insiders access to sensitive information. Consequently, it also means more risk. Are companies technically ready to deal with the future of data use in the organization? It is important to estimate how it impacts your growth as a business.

Tools And Activities That Reduce Insider Threats



Source: 2020 Cost of Insider Threats Global Report – Ponemon Institute Sponsored by ObserveIT & IBM

DATA HAS THREE STATES – ARE ALL PROTECTED?

Transit

When data moves from one system to another e.g. batch updates or backup.

Rest

When data resides in the database or in a file and isn't being moved or used.

These two states are well-protected, because our focus till now has been on **keeping outsiders out**.

- ✓ Application Security
- ✓ Cloud Security
- ✓ Infrastructure Security
- ✓ Identity & Access
- ✓ Data Loss Prevention
- ✓ Encryption
- ✓ Endpoint Security
- ✓ Firewall
- ✓ Network Security
- ✓ Web Security

Use

When data is being used or manipulated by a system or a person.

Point to Ponder

HOW DO WE PROTECT DATA IN USE?

The list of assets under insider threat keeps increasing. We must protect our core IP, source code, patents, customer data, PII, competitive info or assets, technical information, marketing assets, and so forth. Additionally, every year insider threats get only graver with more attacks and exploitations of vulnerabilities.

One of the areas businesses need to focus on are the third-party partners we leverage. As an example, with the recent COVID situation, businesses are acquiring more outsourcing partners to ensure they don't have a single point of failure. Many of these partners have access to sensitive data.

We need to make sure the partners we choose have the right security mindset and controls. They should have a strong culture of compliance and security, communication protocols and change management abilities that we have in in place in our own organizations. I would strongly recommend businesses invest their own time in training not just employees, but these partners and consultants as well.

BEST PRACTICE SUGGESTIONS

01 Monitor behaviors such as downloads, unnecessary data access, files being sent to personal accounts, social media activity, etc.

02 Put tighter controls in place for endpoint protection, intrusion detection and prevention, DLP, PAM, Encryption.

03 Communicate, train and repeat messages that reinforce good behaviors. Ensure employees take courses on code of ethics, non-malicious behaviors. Establish that behaviors are being monitored because "the behavior you pass by is the behavior you accept".

FEATURED EXECUTIVE

Sameer Khera

CIO
Norton LifeLock

> “Monitor behaviors such as downloads, unnecessary data access, files being sent to personal accounts, social media activity, etc.

FEATURED EXECUTIVE

John Hluboky

Principal Security Architect
AllScripts

> “Ensure your data is classified and labelled or tagged. This allows you to focus your efforts where they count the most.

I feel insider threats have been, are, and will continue to be a critical threat to organizations. As we see more emergence of government-backed cyberattacks, compromised or “planted” individuals within an organization are likely. Publicizing these events and reinforcing the patterns of insider threats during security awareness training is key to increasing visibility on this attack modality.

The primary vulnerability stems from people. Take the current COVID pandemic as an example. How many people have very quickly fallen on financial hard times, or face medical emergencies for their families that may not be covered by health insurance? A malicious actor could appear a savior who is throwing a lifeline while we’re drowning.
The need of the hour is educational awareness and user activity monitoring. Leveraging machine learning to rapidly cull through the growing mountain of data and provide actionable alerts with minimal false positives is where the industry is moving.

BEST PRACTICE SUGGESTIONS

01 Ensure your data is classified and labelled or tagged. This allows you to focus your efforts where they count the most.

02 Monitor access to the data and aggregate to a SIEM or data lake.

03 Establish known-good patterns based on data in the SIEM and alert on deviations from this baseline.

FEATURED EXECUTIVE

Hemanta Swain

VP & CISO
TiVo

> “Identify the company’s most valuable assets. Then, perform a risk assessment to assess the risk of data loss or breaches due to insiders.

According to McKinsey, over 50% of data breaches in the past year involved an insider. With the growth of data and data-centric business model, insider threats have become one of the top security risks for businesses. This is now a common question for CISO in the boardroom. Disgruntled privileged users (admins) mishandling their rights could cause serious damage. Also, human error can be more challenging and visible to the external world when using cloud services. We have to protect sensitive data from being exposed accidentally or intentionally.

Consumer privacy advocacy groups have finally managed to get regulations like GDPR, CCPA and SHIELD passed to safeguard consumer privacy. In this new age of data privacy, businesses must understand sensitive and privacy-protected data is used to support business priorities. In many cases, encryption and pseudonymization will not solve the underlying issue of misuse or accidental breaches. There is a need for proper tools, processes and protocols to minimize the risk related to insider cyber threat.

BEST PRACTICE SUGGESTIONS

01 Identify the company’s most valuable assets. Then, perform a risk assessment to assess the risk of data loss or breaches due to insiders.

02 A layered approach is the most effective for insider threat mitigation: enhance your IAM program, roll out multi-factor authentication with proper logging and auditing, verify and enhance your DLP program, and deploy user and entity behavior analytics tools to analyze logs and score the risks.

03 While proactive majors are highly essential, one should be ready to recover from any incident. Be prepared with your backup strategy, process, and proper protocols to act quickly and minimize the impact in case there is any incident.

FEATURED EXECUTIVE

Marc Ariano

Head of Cybersecurity
Vroom

> “Security and threats are consistently evolving. You need to continuously tweak your program.

Protection from insider threats depends on training insiders, knowing the value of the data in question, asking how easy it is to monetize this data, and, of course, discovering the unknown factor of motivation. Along those lines, we should see changes in controls, deterrence, threat response, and bigger adoption in behavioral analytics. Privacy will play a big role around citizen monitoring. Social media, lifestyle, and personal situations can all influence or motivate someone depending on the situation. Certain data classifications may warrant that level of surveillance.

With so much data and so many devices, you have to build out your security program around the crown jewels. Controls that help detect, automate response, challenge, segment, and recover will mitigate the threat from insiders.
Mature awareness programs, polices, and procedures are also needed. This is not a problem that is easily solved with technical solutions and not all actions are intentionally malicious.

BEST PRACTICE SUGGESTIONS

01 Security and threats are consistently evolving. You need to continuously tweak your program.

02 Focus on the data and systems of value and high business impact.

03 Training, training, training. A good security awareness program is engaging, incurs minimal cost, and goes a long way in protecting the environment.

05

ECOSYSTEM SPEAKS

What do sellers, advisors and consultants for security teams have to say about insider threats?

FEATURED EXECUTIVE

Siddharth Bohra

Chief Business Officer - Tech, Media, Consumer goods & Life Sciences; Head - Digital & Analytics
Larsen & Toubro Infotech

> “Businesses need to make security a mainstream conversation and not an afterthought.

There is both a front-end and a back-end reason for the increasing concern over insider threats. In the front-end, the “consumerization” of every industry has led to an all-round increase in data generation. Data is now at the very core of business growth. And on the back-end, every company function is undergoing digital transformation at a rapid pace. Functions like supply chain, field operations, manufacturing, and R&D are undergoing fundamental transformations and becoming much more agile by leveraging data.

Add to these the fact that data is now being stored and analyzed not only in centralized, vaulted data stores, but also on the edge and on employee devices. This implies our vulnerabilities are only multiplying. Businesses need to make security a mainstream conversation and not an afterthought. Also, till now there has been a higher emphasis on external threats. Going forward insider threats will also need to be at the center of attention for security teams.

BEST PRACTICE SUGGESTIONS

01 There needs to be a consistent understanding of security requirements and threats within an organization. An inconsistent security posture leads to the exploitation of security gaps by threat actors.

02 Security teams need to be empowered to move faster when new challenges emerge. The cybersecurity space is extremely dynamic and how quickly your team responds to alerts and situations can make a significant difference to the business.

03 Flip the conversation on security by not just monitoring for vulnerabilities and misuse of data, but also highlighting areas where data can be used more aggressively. Security teams are very well-positioned to help the company become more data-driven.

What makes insider threats more important for security teams is the increased adoption of a cloud-first strategy and data-centric models. While access control, authorization, and SIEM/SOAR-based monitoring are all good steps, security teams will have to go the extra mile to accommodate for the "human element" that pervades insider behaviors.

CISOs have to be torchbearers of a different way to think about security – one that leads with knowledge-based trust instead of championing zero trust. If anything, we have to move over to a world of 100% trust – trust in employees as well as trust our in monitoring, reporting, and remediation capabilities.

We must democratize the use of data without telling individuals what to do or not to do. We must coach and trust insiders while going upstream to observe behaviors and protect data from exfiltration or privacy violation. Most breaches today are because of careless or accidental actions and we need to build reporting and automation capabilities that eliminate the chances of these actions causing long-term damage to the business.

BEST PRACTICE SUGGESTIONS

01 The current approach of centralizing everything and monitoring alerts in SIEM is difficult and manual. We must move towards automation at the very grassroot and operational level. CISOs should demand vendors build automation capabilities and not just reports or alerts.

02 Rather than security training (which is very unidirectional, usually top-down), we need to build a culture of security awareness and consciousness where every employee feels responsible for security, understands risky behaviors and contributes actively to the internal dialogue.

03 For CISOs, in particular, internal messaging and narratives are very critical. They must foster a posture that leads with trust but is also backed by strong automation and remediation capabilities in the event of an incident.

FEATURED EXECUTIVE

Shaq Khan

CEO
Fortifire

> “We must coach and trust insiders while going upstream to observe behaviors and protect data.

06

INSIDER THREATS CHECKLIST

An easy reckoning list from the executives' advice to understand the level of your preparedness against insider threats

INSIDER THREATS CHECKLIST
BY RED BOOK AUTHORS

DATA MAPPING

□ Identify the company’s most valuable assets - the data and systems of value and high business impact

□ Classify data by labelling or tagging them based on value, sensitivity, risk posture, usage levels, etc.

□ Create a 360-view on insider exploitability by identifying data interactions and travel path of the data across the customer journey

□ Identify suppliers, contractors, partners and assess their security best practices, processes, and tech stack

□ Establish and clearly document enterprise-level governance and control policies

□ Tweak the insider threat program at a fixed frequency to address security and threats as they evolve

□ Secure executive backing for the insider threat program

INSIDER THREATS CHECKLIST

BY RED BOOK AUTHORS

STRATEGY & PROGRAM

- □ Establish baselines for secure access, usage, behaviors, etc.
- □ Validate all working assumptions at every engagement and by actively managing trust
- □ Perform a risk assessment to determine the risk of data loss or breaches due to insiders
- □ Ensure that entities do not retain privileges to initiate a trusted action beyond the perimeter of the request that provisioned it
- □ Grant privileges to the minimally viable constituent of the system that will dispose the action
- □ Map out the entire mix of federal, state, and industry regulations and laws that deal with consumer data

INSIDER THREATS CHECKLIST
BY RED BOOK AUTHORS

VISIBILITY & MONITORING

□ Identify behavioral deviations against the organization's established baselines

□ Maintain a complete audit trail of who's accessing what

□ Monitor behaviors such as downloads, unnecessary data access, files being sent to personal accounts, social media activity, query risks, etc.

□ Monitor access to the data and aggregate to a SIEM or data lake

□ Reprioritize threat information to surface most critical alerts based on threat posture

□ Monitor how data is used from structured databases on-prem or in the cloud (because that's where the crown jewels are usually stored)

□ Flag and correlate for simple indicators of what shouldn't be happening

INSIDER THREATS CHECKLIST
BY RED BOOK AUTHORS

TRAINING & CULTURE

□ Establish a robust security awareness program that is engaging, company-wide, and repeated over time

□ Reinforce good behaviors and highlight sample malicious or careless behaviors

□ Put tighter controls in place for endpoint protection (e.g., cutting off access to USB ports)

□ Establish clearly that behaviors are being monitored, so that people know they need to act responsibly

□ Democratize security - make the safety of sensitive data everyone's responsibility

□ Personalize training and content for teams or individuals to explain their role and get them to add value to the process

□ Understand staff temptations especially in teams like Customer Account Setup, Treasury, Accounting, or HR (where a breach can cause high financial damage)

THE RED BOOK OF INSIDER THREATS

SUMMER 2020

Co-Authored By 15 Senior Security & Tech Executives

Proudly Presented By

DASERA

ISBN 2370000818737
2 370000 818737