Insider Threat Report

Out of sight should never be out of mind

verizon
business ready

State of the Insider Threat

Adjusting to a major promotion, a wise colleague once remarked, "Management would be easy if it weren't for the people." The same can be said for cyber risk management. What's more challenging: delivering an annual performance review, or discovering that a valued employee has smuggled valuable digital information through a backdoor? It's easier to navigate conversations about attendance and personal objectives than to conduct investigations into internal data leakage (e.g., Confidentiality), fraud (e.g., Integrity) or sabotage (e.g., Availability) resulting in a reportable data breach or cybersecurity incident.

Nonprofits, commercial organizations of all sizes and industries, and government agencies must all be ready to face cybersecurity threats including data loss, theft, vandalism and service disruptions. External actors – outsiders trying to break into your organization's systems – deserve real defensive effort and attention. But employees and partners can do just as much damage from the inside. Whether from malice or negligence, the results can be equally devastating.

Data Breaches and Cybersecurity Incidents Defined

As we discuss data breaches and cybersecurity incidents, we'll use Data Breach Investigations Report (DBIR) definitions:

- **Incident**
  A security event that compromises the integrity, confidentiality or availability of an information asset.

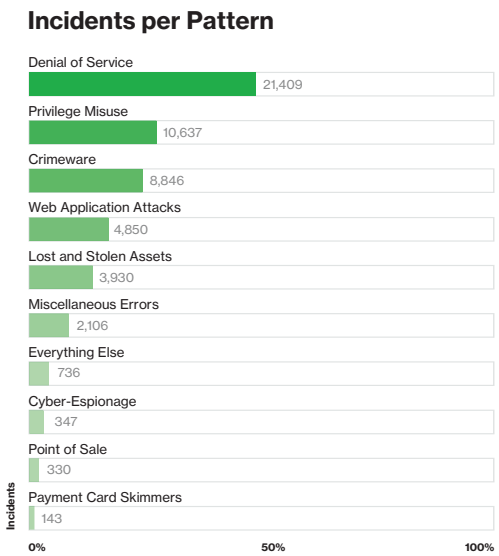
- **Breach**
  An incident that results in the confirmed disclosure – not just potential exposure – of data to an unauthorized party.

VERIS Framework

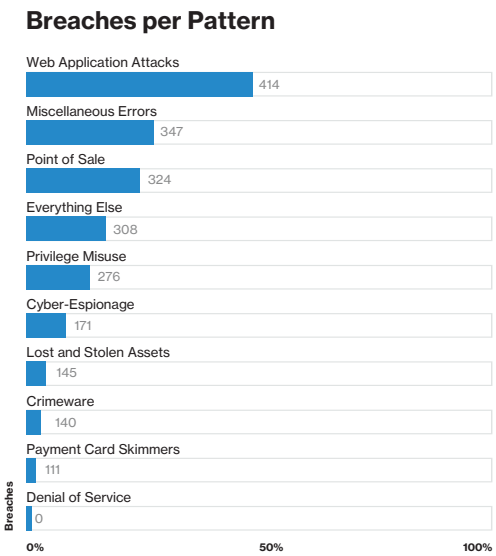
The Vocabulary for Event Recording and Incident Sharing (VERIS) Framework defines threat actors as "entities that cause or contribute to an incident, whether malicious or non-malicious, intentional or accidental, direct or indirect." Threat action varieties most attributable to insiders include Social (human assets are compromised), Misuse (insiders are threat actors) and Error (people making mistakes). If you're interested in learning more about VERIS, check out these resources:

- **VERIS Framework**: veriscommunity.net
- **VERIS Schema**: github.com/vz-risk/veris
- **VERIS Community Database**: github.com/vz-risk/vcdb

The importance of being prepared for both external and internal threats is clear in reading the 2018 Verizon DBIR. With a data-driven overview of data breaches[1] and cybersecurity incidents, the DBIR identifies key incident classification patterns in cybersecurity incidents and data breaches. Internal and external threats are both cause for concern:



2018 DBIR Figure 1. Percentage and count of incidents per pattern (n=53,308)



2018 DBIR Figure 2. Percentage and count of breaches per pattern (n=2,216)

Figures 1–2.
2018 DBIR Incidents per Pattern and Breaches per Pattern

[1] The "n" value in this report represents the number of incidents or breaches. A singular incident / breach can feature multiple varieties of threat actions or other enumerations.

In Figure 1 (above), we see that Privilege Misuse[2] (also called Insider and Privilege Misuse) represents some 20% of all cybersecurity incidents and nearly 15% of all data breaches in the 2018 DBIR. The Insider and Privilege Misuse pattern includes insider threats when external threats collaborate with internal actors to gain unapproved access to assets.

Miscellaneous Errors rank second in the breach pattern column in Figure 2 (above). When trusted insiders don't follow established policies and procedures – such as emailing confidential spreadsheets to their home accounts for weekend work, or faxing personal information to an unconfirmed number – it's clear that insider threat mitigation should be an integral part of every organization's security program.

Insiders have advantages over external actors seeking to circumvent security: insiders often enjoy trust and privileges, as well as knowledge of organizational policies, processes and procedures. They know when logging, monitoring and auditing are used to detect anomalous events and behavior; and that it's difficult to distinguish legitimate and malicious access to applications, data and systems.

Close readers of the DBIR may recall that internal threats are defined as those "originating from within the organization … full-time (or part-time) employees, independent contractors, interns and other staff." For this Insider Threat Report, we'll go a step further in defining insider threats with five Data Breach Digest (DBD)[3] scenarios:

1. **the Careless Worker** (misusing assets). Employees or partners who misappropriate resources, break acceptable use policies, mishandle data, install unauthorized applications and use unapproved workarounds; their actions are inappropriate as opposed to malicious, many of which fall within the world of Shadow IT (i.e., outside of IT knowledge and management).

2. **the Inside Agent** (stealing information on behalf of outsiders). Insiders recruited, solicited or bribed by external parties to exfiltrate data.

3. **the Disgruntled Employee** (destroying property). Insiders who seek to harm their organization via destruction of data or disruption of business activity.

4. **the Malicious Insider** (stealing information for personal gain). Actors with access to corporate assets who use existing privileges to access information for personal gain.

5. **the Feckless Third-Party** (compromising security). Business partners who compromise security through negligence, misuse, or malicious access to or use of an asset.

In this report, we'll discuss victim organizations and affected industries, threat actor misuse varieties and vectors, as well as affected assets and data varieties. In framing countermeasures and the building blocks for an Insider Threat Program, we'll take a two-step approach: first, knowing your assets and people and next, implementing 11 countermeasures to reduce risks and improve responses.

Now, let's look at VERIS data and some scenarios to see what we can learn.

[2] All incidents tagged with the action category of Misuse – any unapproved or malicious use of organizational resources – fall within this pattern. This is mainly insider-only misuse, but outsiders (due to collusion or privileges not disabled) and partners (because they are granted privileges) show up as well.

[3] The Verizon Data Breach Digest (DBD) is a collection of data breach and cybersecurity incident scenarios experienced by our VTRAC | Investigative Response Team. These scenarios illustrate how breaches work, including intrusion vectors, threat actions, and targeted vulnerabilities, as well as countermeasures for mitigating, detecting, and responding to common and lethal scenarios.

VERIS — Breach Discovery

The breach timeline metrics in our DBIRs paint a dismaying picture. External attackers can compromise systems in hours or even minutes, while it can take months or more for organizations to detect intrusions. Since insiders have fewer barriers to overcome and compromises don't require circumventing controls, the time-to-compromise and time-to-exfiltrate metrics for insider threat actions are grim.

This time from an unsanctioned action (such as unauthorized access to a database or email transfer of sensitive data) to discovery represents a vast area for improvement. Most breaches that begin with an abuse of access are only found months or years later. The time-to-discovery for breaches in the Insider and Privilege Misuse category over the last five DBIRs (2014-2018) reflects this:

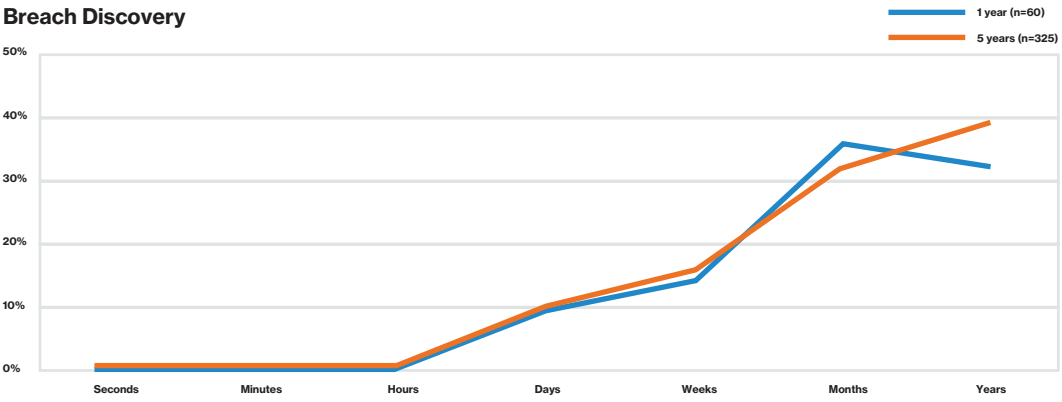


Figure 3.
Breach Time to Discovery within Insider and Privilege Misuse Breaches

Whether culprits start with some level of privileged access or not, few breaches are discovered within days or faster. With financially motivated breaches, the discovery method is usually external. Fraud detection, identifying compromised payment cards, and consumer reporting of identity theft are common ways organizations discover breaches. Over the previous five DBIRs (2014-2018), only 4% of Insider and Privilege Misuse breaches were uncovered using fraud detection, compared to over 20% of the remaining breaches.

Countermeasure – Integrate Security Strategies and Policies

Create an Insider Threat Program that's integrated into the overall security strategy and policies. This strengthens efficiency, cohesion and timeliness in addressing insider threats. Integration should include:

- Risk Management Framework
- Procurement Management System
- Business Continuity Plan (BCP)
- Disaster Recovery Program (DRP)
- Financial and Accounting Management Policies
- Legal and Regulatory Management
- Human Resources (HR) Management
- Security Awareness Program
- Intellectual Property Management
- Software Development Life Cycle (SDLC)
- Project Management

Priority for strategies and policies should be based on risk management, business needs and industry benchmarking.

Personnel Security

We've defined insiders as full- and part-time employees, independent contractors, interns and other staff, as well as business partners and third parties with some level of privileged access. Human resources controls, security access principles, training and third-party management controls can mitigate risks.

Human Resources Controls

Establish and periodically review HR processes including job descriptions, contract details, hiring, onboarding, disciplinary actions and termination.

- **Job Descriptions**
  Create clear job descriptions that detail tasks, responsibilities and requirements for accessing systems. Senior leadership should approve descriptions.

- **Contract Details**
  Ensure individual and organizational contract details delineate information security roles and responsibilities. Obtain signed Non-Disclosure Agreements (NDAs).

- **Hiring Process**
  Vet prospective employees through background checks and comprehensive screening interviews. Perform sound pre-employment checks for job applicants. Depending on the sensitivity of the position, these should include identification, education, previous employment and financial and criminal background checks as applicable (e.g., Europe, Japan). Obtain signed NDAs.

- **Onboarding Process**
  Conduct cybersecurity training as part of new hire onboarding. Issue equipment. Obtain signed Acceptable Use Policies (AUPs) and renew these AUPs annually.

- **Disciplinary Process**
  Develop a disciplinary process for situations involving security breaches caused by employees and others with inside access.

- **Exit Process**
  Develop a formal process covering voluntary and involuntary termination. Include exit interviews, user account termination and employee-issued property (e.g., laptops, equipment, badges) return. Establish provisions remaining valid for a certain period after termination (e.g., non-compete agreement, NDA).

Security Access Principles

While threats from unscrupulous or disgruntled employees may be unavoidable, there are methods to limit damage. Our investigative experience confirms industry best practices to prevent and mitigate insider threats through mandatory leave, job rotation, duty separation, least privilege and "need-to-know."

- **Mandatory Leave**
  Require mandatory leave throughout the year. This serves as a deterrent and detector (e.g., a coworker covering for a vacationing colleague could discover and deter unauthorized activity).

- **Job Rotation**
  Periodically rotate job functions. This can deter and detect inappropriate behavior and provides the added benefit of skills cross-training.

- **Duty Separation**
  Separate duties, especially for sensitive or shared processes and tasks. This ensures no individual can complete a single task (e.g., dual password control).

- **Least Privilege**
  Only assign access privileges minimally necessary to perform a task. This limits unauthorized or unintended actions. Make sure access reflects any role changes.

- **"Need-to-Know"**
  Only grant access necessary to perform a job or function. This limits exposure of sensitive data and devices such as trade secrets, customer data and proprietary information.

Terminating User Accounts

Upon notification of an employee or business relationship termination, take these actions:

- Disable user accounts; remove accounts from Active Directory
- Terminate remote access (e.g., virtual private network (VPN))
- Terminate remote web, mobile and other tool access
- Terminate email account access; remove from distribution and group lists

Security Awareness Training

Employees are the first line of defense when combating many incidents, including insider threats. Security awareness training for new employees, seasoned workers, management and part-time employees reinforces what is and what isn't acceptable. Training should have full management support and tracking attendance or completion is recommended.

Start on an employee's first day as part of onboarding and conduct at least annual refresher training and assessment sessions. Supplement training throughout the year with emails, login banners, desktop background reminders and awareness posters in workplace common areas. Training should include:

- **Policies and Procedures**
  What these are and why these have been defined. Review all current cybersecurity policies associated with employees, including acceptable use, BYOD, information security and physical security.

- **Topical Security**
  How to spot social engineering attempts, how to recognize insider threat indicators and how/when to report suspected security issues.

- **Acceptable User Behavior**
  What is and what isn't acceptable.

- **Disciplinary Consequences**
  What the consequences are for unauthorized or malicious activity.

Drive compliance by obtaining online or written acknowledgement of responsibilities for reporting suspicious behavior. Help employees recognize and report potential indicators of insider threat activity. Establish an open door, anonymous or confidential policy for reporting insider threat incidents to management, HR or other designated groups.

Preparing for Organization Changes

Be ready for the impact of organization changes including transfers and promotions. Maintain strict "need-to-know." Coordinate restructuring and job movement with HR and management. Establish a termination protocol covering notification timing, device disabling, as well as network and physical access removal. Safeguard employee devices for a defined time after termination.

Educate employees on indicators of potential insider threat activity involving coworkers or business partners, such as:

- Consistently working outside normal hours (e.g., when nobody is around).
- Exhibiting patterns of security violations (e.g., repeatedly circumventing protocols by using unauthorized USB flash drives).
- Attempting to access data, systems, or facilities without a valid reason (a “need-to-know”).
- Commenting on intent to steal or destroy data.

Countermeasure – Implement Personnel Security Measures

Measures to mitigate cybersecurity incidents for employees and others granted enterprise access include:

- **Human Resources Controls**
  These span job descriptions, contract details, screening and hiring, onboarding, disciplinary process and exit process.
- **Security Access Principles**
  These include job rotation, duty separation, least privilege and “need-to-know.”
- **Security Awareness Training**
  Topics include policies and procedures, acceptable use and potential disciplinary consequences.

Third-Party Management Controls

The DBIR defines partners as any third-party sharing a business relationship with the organization. This includes suppliers, vendors, hosting providers, outsourced IT support and more. Some level of trust and privilege is usually implied between business partners. Besides HR Controls, we advise implementing additional controls for vendor management.

Implement a Procurement Management System to track and control vendors and contract requirements. Make these requirements measurable and use contractual leverage for not fulfilling security requirements. Within these requirements, beyond Personnel Security Principles, implement these controls:

- Use controlled workspaces for deterrence, prevention and monitoring.
- Implement a secure corporate email system; prohibit using personal web mail accounts for business.
- Periodically review, reconcile, manage, and monitor all third-party account access to networks, systems and applications.
- Identify and monitor highest-risk third-party user accounts.

Focus on critical controls for high-risk situations to help reduce violations and failures. Identify high-risk situations by assessing factors including: highest risk access and highest attrition vendors, high-spend contracts, overleveraged third parties and geographic distance. Ensure you have the capability to identify and address any insider threat issues. Finally, consider the further step of embedding cyber-trained, credentialed security personnel in high-risk environments.

Cloud Storage Data Collection Challenges

While cloud storage solves many issues, it also poses new challenges. Many organizations benefit from moving local IT functions to the cloud, but in doing so, they lose the control of having their own servers with employees responsible for security.

Organizations must have a documented process to extract data wholesale from a cloud environment – whether unstructured data (such as file level backups), structured data (such as databases) or entire virtual machines.

Simply downloading this data may not be practical: a hard drive may require transport or a data center could require a visit. Organizations should make sure cloud services providers are contractually obligated to help with this process; a Service Level Agreement (SLA) should dictate this.

Finally, it's been said a backup isn't successful until it's been restored once. Organizations should assume their cloud services provider won't release your data until you've retrieved it at least once in a Disaster Recovery Plan (DRP) exercise or data breach simulation.

Scenario #1 — the Careless Worker

The careless worker is one of the more difficult threat actors to defend against. Their actions include mistakes, misusing assets and credentials and using unapproved workarounds.

The Situation[4]

We are a growing technology consulting business and we recently won a major contract requiring us to quickly hire technical staff. The award generated substantial good press for us and we received numerous inquiries from talent interested in joining our organization.

As an HR Manager, I know that rapid hiring often leads to hiring candidates who appear great on paper but fall short in applicable skills. I've also seen highly qualified candidates overlooked because they're intimidated by traditional job interviews. Accordingly, I suggested we host an online "hackathon" event to assess technical skills in near real-time and identify quality candidates.

We have many virtual teams across the country collaborating on projects. I decided the hackathon would require candidates to work in groups, so we could assess technical and teamwork skills as we sought to hire project managers, business analysts, network architects and information security analysts.

After reassuring management that a hackathon isn't actual "hacking," the idea was embraced and I was asked to lead the initiative. We engaged our Information Technology (IT) team to help HR set up the event. The IT team proposed using a web application that would take nearly three months to design, test and implement. We let them know we only had two weeks. After initial pushback, the IT team agreed and quickly set to work.

Over the next two weeks, I worked with our external recruiting agency to develop a list of candidates to invite. The theme would be "Technology to Improve Business and Personal Productivity" and the goal was helping our employees address work-life balance.

The IT team designed and tested the web application. The app included hackathon project questions and an online registration form that saved candidate details to a database. HR and management approved the app and we went live with registration the next day.

The hackathon was an enormous success, resulting in multiple hires. A few days later, though, I received an alert on my mobile phone: "Confidential – Web Application Data Breach Incident." Our Chief Information Security Officer (CISO) was calling an Incident Response (IR) stakeholder meeting.

[4] This scenario was published originally as the stand-alone DBD scenario "Web app attack – the Tuple-Row Honey" (https://enterprise.verizon.com/resources/).

Investigative Response

The IT security team had detected significant inbound traffic accessing the web application server, along with several anti-virus (AV) detection alerts. We engaged the Verizon Threat Research Advisory Center (VTRAC) | Investigative Response Team and they were on their way to investigate.

The IR stakeholder meeting attendees included our General Manager, a General Counsel Representative, the CISO, the IT security team, the IT team who'd worked on the hackathon web application, two VTRAC investigators and me.

The CISO started by informing us that our "Hackathon Talent Search Event" was the apparent source of a cybersecurity incident and later Personal Identifiable Information (PII) data breach. I couldn't believe what I was hearing. We'd taken precautions to vet the candidates. I blurted out, "Why'd they go and cause this trouble on our systems when they were looking for an employment opportunity with us?"

At this point, the General Counsel Representative leaned forward, asking, "So, let me get this straight. You're saying we've got a breach of PII on our hands here?!"

The VTRAC investigators went to work with the IT security team and determined that the incident wasn't caused by a job candidate, but rather by a malicious attacker who'd discovered the web app server and exploited a vulnerability.

The vulnerability was described as a remote code execution attack. The investigators determined that an outdated version of the web application framework had been used and that a web application firewall (WAF) wasn't in place. Several web shells allowing remote access were discovered on the server. The attacker accessed these web shells prior to their detection and quarantine by the installed AV software.

The investigation also discovered signs of remote logins and successful database queries on the job candidate database. Finally, the logs indicated the attacker had plundered the data, including the candidates' personal information.

Since the attacker accessed PII data, we had a legal obligation to notify several states' attorneys general and the affected individuals. I immediately worked with our Legal and Executive Management teams to craft data breach notification letters, create holding statements and tailor our corporate messaging to address this unfortunate event.

The IT team knew the web application was running an outdated framework and had been planning to upgrade it after the first hackathon. Given that the invite was sent to a handful of vetted individuals, they assumed it would be okay to briefly run the vulnerable application without a WAF. Fortunately, they had segmented the web application from the corporate network, reducing the potential for additional data exfiltration.

Lessons Learned

The big lesson learned was that once a server is on the Internet, it's there for all to see and access – not just invited individuals. IT security teams must be active in all projects, not mere afterthoughts. It's crucial not to rush development without considering organization-wide security.

Mitigation and Prevention

- Develop web apps based on industry best practices; follow the Secure SDLC; incorporate information security throughout the life cycle.
- Scan web apps for vulnerabilities; perform periodic penetration tests; develop a patch management program to swiftly patch and update identified vulnerabilities.
- Set host-based and enterprise AV solutions to be continuously updated with the latest engine and virus definitions.
- Install WAFs, a File Integrity Monitoring (FIM) solution, and host / network Intrusion Detection Systems (IDS); maintain enough logging.
- Implement proper data segregation and network segmentation, especially with critical data and systems.

Detection and Response

- Assemble the IR Team; include stakeholders relevant to the specific cybersecurity incident; engage law enforcement at the right time and with advice from legal counsel.
- Engage a qualified and experienced digital forensics firm for investigative response activities including malware analysis, endpoint forensics, network forensics, threat intelligence and containment and eradication support.
- Collect and preserve evidence; use vetted tools and procedures for evidence collection and preservation; potential evidence includes volatile data, hard disk drive images, network packet captures and log data.
- Leverage established and documented evidence handling procedures; use evidence tags, chain of custody forms and an evidence tracking log to secure, preserve, collect and store evidence.
- Prepare public relations responses for various data breach scenarios ahead of time; adjust the response to specific circumstances.

Deterring Insider Threat Activities

Effective security policies and standards can deter insider threats. Policies should include acceptable use, Bring Your Own Device (BYOD), information security and physical security. Conduct annual information and physical security training for all employees. Use login banners, screen savers and desktop backgrounds to remind users actions are being monitored and policy violations are flagged. Consider publishing anonymized security violation statistics.

Threat Actors

Verizon's DBIR defines Insider and Privilege Misuse as trusted actors leveraging logical or physical access in an inappropriate or malicious manner. This is mainly insider-only misuse, but outsiders (through collusion) and partners (via granted privileges) also show up in the dataset. Internal threat actors operate from a position of trust, which they use to steal, corrupt or destroy data, disrupt business operations or embarrass an organization. Insider threats include full- and part-time employees, interns, business partners, contractors and outside service providers.

VERIS — Actor Varieties

Reviewing our DBIR Insider and Privilege Misuse data for internal threat actor varieties over the previous year (2018), we see Other (30.8%), End User (30.1%), Doctor or Nurse (16.0%), and Manager (5.8%) as the most prevalent actors. Nearly 61% of internal actors are defined as "Other" or "End User" and aren't in positions granting them a higher level of access or stature to influence. The top 10 threat varieties within Insider and Privilege Misuse for 2018 and for the previous five years (2014-2018) are:

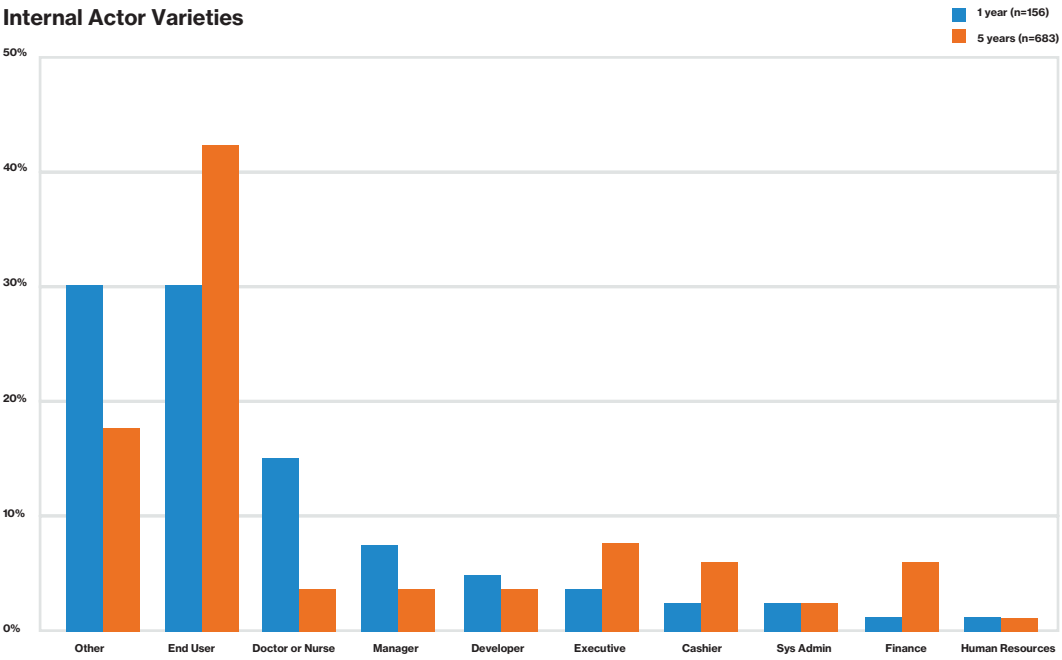


Figure 4.
Internal Actor Varieties within Insider and Privilege Misuse Breaches

The VERIS Framework establishes varieties or roles of internal threat actors. The question we are attempting to answer is: how often are roles with higher user privilege (e.g., System Administrators), access to monetizable data (e.g., Cashier / Bank Teller / Finance) or privy to sensitive corporate strategies/plans (e.g., Manager or Executive) responsible or involved in data breaches?

Interestingly, this quote from the 2013 DBIR remains relevant: "Data theft involving programmers, administrators or executives certainly makes for interesting anecdotes, but is still less common in our overall dataset than incidents driven by employees with little to no technical aptitude or organizational power." Regular users have access to sensitive and monetizable data and are behind most internal data breaches.

Dark Web Monitoring

Dark web monitoring tracks cybersecurity threats and activities on the hidden Internet. Many companies have programs to detect and anticipate these threats, using tools and techniques to infiltrate cybercriminal activity hubs. These include black markets, where stolen data and other information on organizations or employees is sold. Also included are social sites and forums where users can post and reply to topics. Finally, these include dump sites, such as Pastebin, where anonymous people can post information including confidential documents, emails, databases and other sensitive data.

Enterprise Threat Hunting

Organizations must now assume that external attackers are already inside their network. Cyber threats continue to evolve, ranging from off-the-dark-web malware and ransomware to more complex and targeted threats. It's crucial to detect these threats quickly to reduce the risk of valuable business assets being compromised.

A key aspect of enterprise threat hunting is using high-quality data and sound strategies to start the process. The process can be analyst-driven or assisted by machine learning technology. Focus areas for threat hunting include log management and correlation, full packet capture, endpoint detection, honeypots, as well as IDS and other network and security infrastructure.

Many organizations are struggling with cybersecurity efforts because of a daunting worldwide InfoSec talent shortage. Autonomous threat hunting can decrease dependence on human analysts, with accurate and comprehensive security solutions that support and augment human staff.

Maintaining a proactive approach to threats can prove the best defense.

Countermeasure – Conduct Threat Hunting Activities

This includes periodically searching to detect and investigate risks inside and outside the enterprise. Leverage intelligence for actionable insights. Intelligence sources should include:

- **Open-Source Intelligence (OSINT)**
  Intelligence derived from publicly available sources (e.g., the Internet).
- **Dark Web Monitoring**
  Knowledge gained regarding activity on the restricted and hidden Internet.
- **Cybersecurity News Feeds**
  Insights from open source media broadcasts and articles.
- **Knowledge-Sharing Partners**
  Information from industry-related groups (e.g., Financial Services - Information Sharing and Analysis Center (FS-ISAC); Payment Card Industry (PCI) Security Standards Council (SSC); and government entities (e.g., FBI Private Industry Notification (PIN), national governmental CERT).
- **Cybersecurity Incidents**
  Historical record of incidents and events detected, responded to, and investigated; includes applied containment, eradication and remediation measures.
- **Enterprise Detection and Response (EDR) Solutions**
  A unified capability for cybersecurity and incident response tasks that span monitoring, detection, alerting, investigating and mitigation.

Threat Intelligence

When something is wrong, people often try to mask their emotions. But they usually show signs such as changes in behavior, whether their distress is personal, professional or psychological. Too often though, it's only after an incident that such personal issues are recognized as motivators.

Whatever the work environment, someone near the at-risk employee likely witnessed something at one point. They may have ignored signs, not added things up or not cared enough to mention anything. One way to combat missed signs is through indicator bubbles – spheres of seemingly unrelated employee changes. These can be grouped together to identify potential issues.

Potential Indicator of an Insider Threat – Elicitation

Elicitation is a technique to discreetly gather information, used by a skilled collector in a seemingly typical social or professional conversation. Victims (elicitees) may never realize they were the target of an attempt to obtain meaningful information.

To be ready for this threat, it's important to understand how elicitation works. Often, an elicitee has some of these characteristics:

- Desires to appear well-informed
- Tendency to gossip
- Desires to be appreciated and show they have something to contribute
- Tendency to correct others
- Believes others are honest
- Is prone to showing off

On the other side of the equation, an elictor tends to have these characteristics:

- Pretends to know of associations in common with the elicitee
- Feigns ignorance of a topic
- Exploits the elicitee's instinct to complain or brag
- Uses flattery and appreciation as psychological tools
- Obliquely introduces topics in order to gain insight
- Deliberately says something wrong, hoping the elicitee will offer a correction

Taken alone, an indicator could have normal, natural causes. It's important to understand that a single indicator, or even multiple ones, doesn't mean your employee is an active insider threat. But they can indicate something is wrong and that more attention could enhance the employee's well-being – and thus the organization's. These indicator "bubbles" may surface individually. When viewed collectively, these can indicate insider threat activity.

Figure 5.
Insider Threat Indicator Bubbles

Countering this threat through organization-wide situational awareness training is vital to ongoing security efforts. Security is the responsibility of all employees, not just IT security teams. All employees should be encouraged to report suspicious activity, which can include insider threats. Dedicated intelligence teams can also be created to detect and report on these types of threats.

Many organizations conduct drug screening, background investigations, and data collection (e.g., social media checks, credit history, etc.) when hiring new employees. These checks shouldn't be a one-off event; instead, they should be conducted periodically throughout an employee's career.

VERIS — Actor Motivations

Another way of considering insider threats is to assess activity as intentional or unintentional. Unintentional insider threats can be as impactful as intentional ones.

Unintentional actions result mostly from employees making mistakes at work. An error may happen while hastily redeploying a firewall in a production environment or emailing data to the wrong recipient. There are many reasons for mistakes and they can never be completely prevented. Such unintentional incidents fall into Other Incident patterns[5] and aren't in-scope for this report. Also, by definition, such incidents don't have a motive.

Potential Indicator of an Insider Threat – Requesting Access to Information Outside Normal Job Duties, Including Sensitive or Classified Information

Small business employees typically perform general and varied duties, while most employees in larger organizations have more specific roles. Small and large business owners alike should know the essential functions and typical duties of each employee. This allows easier identification of potential insider threats.

Further, employees should be aware of conduct by colleagues, which could merit more scrutiny and reporting, including:

- Asking others to obtain access to restricted, sensitive information they're not authorized to view.
- Undue curiosity about information not within job scope or "need-to-know."
- Retention of classified, proprietary, or sensitive information obtained during previous employment, without the authorization of that employer.
- Extensive and unexplained use of copier, fax, or computer equipment to reproduce or transmit sensitive, proprietary material.
- Unexplained affluence or lifestyle inconsistent with relative income level, such as sudden purchase of high-value items or unusually frequent personal travel.

[5] Unintentional actions that lead to incidents and breaches are typically categorized in the Miscellaneous Error or the Lost and Stolen Assets pattern.

Intentional actions from insiders, whether malicious or inappropriate, have a motive; we record motives in our dataset whenever they're discernable. Different motivations drive insiders to become threat actors. Most significant are financial gain or revenge (against the employer or colleagues). Intentional insider threat motivations include:

Motive	Examples
Financial: Financial or Personal	Seeking monetary gain for financial problems; being susceptible to monetary rewards or blackmail to engage in malicious activities gain.
Fun: Fun, Curiosity, or Pride	Accessing medical records of patients out of curiosity, not to commit identity theft; breaking acceptable use policies by visiting inappropriate websites; using admin privileges to access employee emails.
Espionage: Espionage or Employment at a Competitor	Using stolen data for future advantage (e.g., starting a competitor or taking employment at a competitor) as opposed to quick financial gain.
Convenience: Convenience of Expediency	Downloading sensitive data to a USB drive for working at home; using unauthorized software or configuration changes to make duties easier.
Grudge: Grudge or Personal Defense	Seeking revenge over perceived mistreatment by management or colleagues; retaliating against management or desiring to damage the organization.
Ideology: Ideology or Protest	Having a fundamental opposition to an organization's practices or mission.
Fear: Fear of Duress	Fearing layoffs or other organizational changes; feeling duress from a superior to act inappropriately or maliciously.

Table 6.
Threat Actor Motives Defined

Reviewing our 2018 DBIR data, we see that the top threat actor motivations were Financial (47.8%), Fun (23.4%), and Espionage (14.4%). The seven threat actor motivations within Insider and Privilege Misuse for 2018 and the previous five years (2014-2018) are:

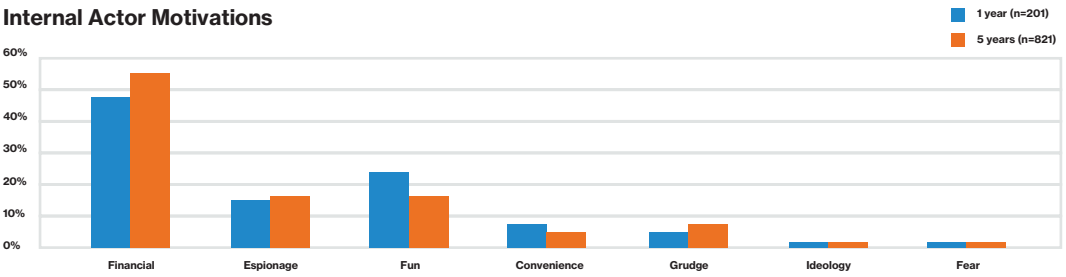


Figure 7.
Internal Actor Motivations within Insider Privilege and Misuse Breaches

In viewing different motivations by actor type – internal, external, and partner – we gain further insight into threat actor motivations for the previous five years (2014-2018):

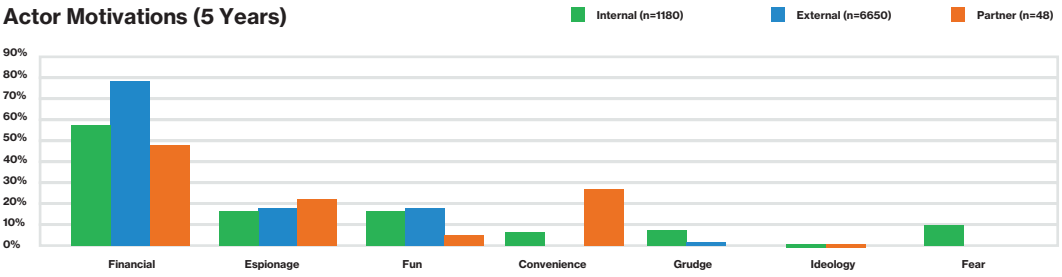


Figure 8.
Actor Motivations within Insider Privilege and Misuse Breaches

Most people behind data breaches, whether insiders or not, are motivated by money; historically, this has been the primary driver for compromising data. We see similar percentages of data breaches associated with the espionage motive. A common scenario here is the exfiltration of internal data or intellectual property for a new endeavor.

Fun (including curiosity and pride) is an interesting motivator. A lone hacker may compromise an organization's data just to show they can. Out of curiosity, a healthcare worker might snoop medical records of patients not in their care, or an employee could access a criminal database to check on a relative or acquaintance.

Behavioral Analysis

Insider threat detection tools are often signature-based. These techniques (such as watch list IP addresses, hash signatures, specific strings in packets, etc.) are useful, but may be analogous to reading yesterday's news. Consider supplementing them with behavioral anomaly detection methods.

Behavioral anomaly detection provides a proactive view into the current environment (like anticipating tomorrow's news). Understanding the drivers behind network anomalies can help proactively identify insider threat trends before they cause major problems.

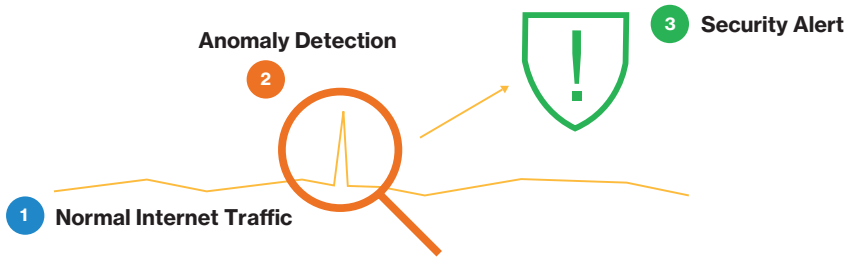


Figure 9.
Behavior Anomaly Threat Detection

Our investigations uncovered examples of behavioral analysis detecting potential insider threats:

Malicious Insider
We uncovered an internal device performing targeted (e.g., NetBIOS, Secure Shell (SSH), Hypertext Transfer Protocol (HTTP), remote admin, ports, etc.) scans across a network segment. Investigation confirmed the device wasn't an authorized corporate scanner. This raised concerns that an internal employee was seeking access to unauthorized infrastructure.

Careless Worker
We detected a broad range of customer devices sending unusual small packets to several Microsoft Azure IP addresses. The Microsoft Azure IP addresses had recent reputational histories of hosting phishing sites such as a fake PayPal site and Microsoft web mail site. The concern was that many employees were phished via email or SMS and enticed to enter credentials in the bogus web sites.

Another Careless Worker
We identified unusually large two-way traffic between a customer device and multiple ISP IP addresses over a well-known port for hosting Xbox online gaming services. Employees were consuming bandwidth for non-business purposes, exposing corporate assets to security risks.

Monitoring and Logging Activity

Enhance logical access controls by restricting, monitoring and logging logical access to sensitive systems and data. This includes critical network segments, network devices, servers, workstations, as well as key accounts, applications and files. Establish baselines for normal user account behavior and network activity and then monitor and log-review for suspicious events:

- Increase configuration change logging and alerting, to include user account creation and modification.
- Create and monitor alerts related to abnormal authentication events, such as numerous password resets in brief periods and access from foreign sources.
- Implement robust access controls and monitoring and logging policies for privileged user accounts.
- Periodically review logs of accounts accessing critical and sensitive systems to detect unusual or elevated account activity.

Use a SIEM solution, or better yet, a User and Entity Behavior Analytics (UEBA) solution to monitor, detect, and log suspicious user account activities. To ensure preparedness, test logging and monitoring systems to verify the required data exists and can be used if an attack occurs. If a data breach occurs, review user account, application, system, and network logs to determine the extent of the compromise and to identify other assets that may have been targeted.

Using NetFlow for Baselining "Normal" Network Behavior

Many organizations use NetFlow for reporting and post-event analysis. But NetFlow can also be leveraged to build a baseline of typical network behavior – then detect new security events in near real-time.

For near real-time, network-based, anomalous behavior detection, seek anomalous behavior in NetFlow data rather than relying on signatures. Understanding the drivers behind network anomalies can help teams proactively identify threats before they become major problems.

Countermeasure – Implement Network Security Solutions

This includes implementing network perimeter and segment security solutions for network traffic monitoring, capture, and analysis. These solutions should include:

- **Network-Based Firewalls**
  Software or hardware security system for monitoring and controlling incoming and outgoing network traffic based on predetermined security rules.
- **Network IDS**
  System for analyzing packets and alerts (passive) on suspicious network activity.
- **Network Intrusion Prevention System (IPS)**
  System for analyzing packets and blocking (active) suspicious network activity; active form of IDS; typically possesses a subset of IDS rules and coexists with IDS.
- **Web Security Gateway**
  Solution based on security zones and data classification for preventing traffic, such as unwanted software and malware, from entering or exiting the enterprise environment.
- **Email Security Gateway**
  Service or device for providing email content filtering or analytics.
- **Data Loss Prevention (DLP) Solution**
  Tool for preventing data exfiltration in two states: Data In-Use DLP, which monitors endpoint data with which users are interacting, and Data In-Motion DLP, which monitors traffic data from endpoint to endpoint.
- **SIEM Solution**
  Tool for reviewing aggregated log data from network, security device, systems and applications for suspicious or anomalous system activity.
- **Segmentation**
  Strategy for segmenting network and segregating data, especially with critical systems and data for security, access and monitoring purposes.

Monitor and then alert upon suspicious network traffic, such as unusual off-hours activity, volumes of outbound activity and remote connections. Leverage a SIEM capability to monitor insider threat activities. Periodically update detection rules and watch lists.

Scenario #2 — the Inside Agent

When inside agents hide their true intentions, it can be difficult to detect their malicious behavior. They typically work on behalf of an external threat actor and secretly steal information for them.

The Situation[6]

Contractors such as auditors and janitorial staff can be nearly invisible in large corporate environments. A purposeful stride or prop of authority such as a clipboard or even a mop can enter virtually anywhere. Some contractors can access broader, more varied areas than a typical employee. Accordingly, a contractor given an economic or vengeful incentive can become a potent threat vector.

Most employees have little awareness of operational changes involving vendors, service providers, or contractors. These details, hidden away inside HR and Accounting departments, focus on keeping the organization running. So it was unsurprising when neither I nor the rest of the IT security team had any idea about problems brewing with our contracted janitorial service. The contracting organization had announced a unilateral pay cut for all employees, revealing this mere weeks before the holiday season.

Even if we'd known of these contracting changes, few would have guessed that a malicious individual offering "bonus pay" would approach the increasingly emotional and desperate janitors. The task was easy: simply carry a USB flash drive in each day. Plug it into a system. Get paid. Feelings of retribution toward the contracting organization, mixed with financial strain, were enough to convince more than one janitor to accept the cover story.

The janitors, hidden in plain sight, had access to nearly everything and quickly compromised multiple systems without arousing suspicion. The infected systems would likely have remained hidden for weeks or months if an alert administrator hadn't noticed unexpected command shell pop-ups upon logging in. A brief investigation showed these tasks were running under a local administrator account and didn't seem related to any legitimate business activity. After adding notes to a trouble ticket, he went on to other tasks.

[6] This scenario was published originally as the DBD scenario "USB Infection – the Hot Tamale" (https://enterprise.verizon.com/resources/).

Investigative Response

This is where I entered the situation. As an internal investigator, I'm tasked with figuring out what it all means. Are these system artifacts malicious? Are these left over from previous configurations? Ultimately, how did this get there? My organization wanted answers.

The first task was to establish a footprint of systems affected by the attack. This list would help guide me to determine the initial infection vector. Having met with the IT security team to understand the artifacts, I pulled domain and system logs from the initially identified workstation. These artifacts turned out to be what are called Indicators of Compromise (IoCs), common ways of locating additional systems affected by a known piece of malware.

Searching through the domain logs with these IoCs in hand, I was able to quickly identify several other systems, each of which had been accessed by the same local administrator account within the same timeframe as the suspect system. This correlation expanded the investigation to include systems beyond the one originally anticipated.

With the larger list of systems enumerated, I presented my preliminary findings to our HR and Legal teams and identified various options. The decision was made to call in the VTRAC | Investigative Response Team to conduct digital forensic analysis on this system, and determine to the extent possible the nature of the malicious activity. The VTRAC investigators forensically imaged the in-scope systems. These images were subjected to multiple types of review, ranging from analysis of the Windows Registry hives to examining system log files and reviewing the shortcuts for suspicious linkages.

Analysis of the systems' logs revealed suspicious command line activity and exploitation attempts, as well as subsequent, unsuccessful cleanup attempts. Interestingly, these same logs showed a USB device driver being loaded onto the system just prior to these exploit attempts. Based on serial numbers in the Windows Registry and other artifacts, it was determined the USB device was a cheap flash drive indistinguishable from dozens of others.

Employing Additional Access Controls

- Disable unauthorized / restrict access to removable media (e.g., USB flash drives).
- Restrict (and monitor) cloud-related data transfers.
- Restrict File Transfer Protocol (FTP) / Secure File Transfer Protocol (SFTP) data transfers.

In our organization, there's an official policy against such devices, but it's rarely enforced. The problem with USB devices in corporate environments is that once a device is plugged in, it could force system configuration changes or allow unauthorized programs to run. This could then allow many other actions. I believed this potential threat and suspicious timing merited further review.

An artifact showed a USB device had been connected to the system, but the central question remained: who connected it? Armed with date-time stamps relating to the USB device, I met with the team responsible for overseeing physical security of the organization's facility. I hoped we might track physical access to the system during the relevant timeframe. To my elation, they informed me badge access was required for the room where the system was located.

I was very eager to see these logs! The Director of Physical Security produced them for me. I found there wasn't much access to the room around the time the USB device activity was identified. The only thing that stood out was the janitorial staff doing their cleaning rounds. It took some time but I finally had the key insight. Could a janitor be my primary suspect? Could they have been plugging something into that workstation? I thought we should ask.

Our HR Department and physical security team interviewed the janitor concerned, and they admitted to plugging the USB device into multiple systems. These systems and timeframes matched identically with my log review and the VTRAC investigators' analysis results. With the technical portion of the analysis complete, I sat back and watched as our HR Department continued to interview the janitor. He expressed remorse, but explained that the upcoming pay cuts would have caused extreme difficulty for him and his coworkers. The prospect of additional holiday spending money and a lack of understanding about the potential for damage led them down a path they couldn't reverse.

Lessons Learned

The janitor was terminated and the exploit attempts ceased. Further review indicated the activity was caught before the threat actor could extract privileged information. Remediation included increased monitoring of IoCs and cleaning up the affected systems. Future mitigation was implemented by changing logging and centralizing hardware devices across sensitive and restricted systems.

While there were digital components to this breach, the biggest takeaway is the importance of physical security. Direct access to a device can circumvent many security controls. Access to USB ports can allow bad actors to load malicious software when a device is rebooted in safe mode or has its drives removed to bypass password security. These technical and physical considerations substantially impacted this case study:

Mitigation and Prevention

- **Establish USB device access / AV policy**
  Host-based enforcement limiting USB device port access could have stopped this attack. Certain organization-provided devices could be whitelisted to not completely remove functionality. Host-based AV can scan any media newly connected to a workstation or device.

- **Disable auto-run functionality**
  IT teams capable of remotely updating system configurations should disable auto-run on non-affected systems to limit potential spread of USB-based infections.

- **Enhance host-based logging and alerting**
  If not for the vigilance of a systems administrator, this incident might have gone unnoticed long enough to inflict serious damage. The physical vector often creates some network noise in which similar activity is discovered. Here, logs were present for systems, but there was no alerting functionality triggered on suspect activity.

- **Leverage network access controls**
  In this scenario, the adversary was defeated early in the reconnaissance stage. However, the organization employs a relatively flat network design, so systems may have expanded accessibility to sensitive systems. Implementing network access controls made it harder to use less secure systems to compromise more secure ones.

- **Set up physical access alerting**
  Access cards allowing limited access to certain areas secure many offices. However, it's trivial for a card to be stolen or cloned. Alerts were created and monitored to look for consistent access patterns, such as an employee's badge being used several hundred feet from their last scan within a short timeframe.

Detection and Response

- **Review physical security access controls**
  Badge readers, security cameras, and sign-in logs shouldn't be ignored; these can reduce suspicious activities requiring investigation.

- **Use an EDR solution to identify affected systems**
  Once an affected system is identified, disk forensics paired with an EDR solution can allow a direct view into additional systems that may be affected.

- **Review network and application logs**
  Review logs related to compromised systems or user accounts to determine other assets that may be targeted.

- **Conduct personnel interviews**
  Interviewing employees, contractors, or other people with access to affected devices can help identify suspicious behavior. These interviews may uncover otherwise unexpected events on affected systems, which can provide investigative leads for forensic investigators.

Payment Card Industry Data Security Standard – Mitigating Insider Threats by Enhancing Data Protection Controls

It takes just one person going rogue to render security controls ineffective and compromise sensitive data. It's common for insiders – employees, contractors, and third-party suppliers – to have access to restricted systems and data as part of their everyday job functions or even inadvertently. While insider threats can never be eliminated, organizations can reduce risks by maintaining a healthy control environment, strengthening control effectiveness through deliberate design, and actively managing security controls year-round. For the PCI environment, this is where the PCI Data Security Standard (DSS) comes into play.

How have organizations performed in keeping controls in place? An analysis of 237 confirmed payment card data breaches investigated by the VTRAC | Investigative Response Team from 2010-2017, across 35 countries, provides a good indicator of how well organizations have maintained sustainable control environments. At the time of a data breach, typically fewer than one-third of organizations were complying with any particular PCI DSS key requirement and none met all requirements:

Trend[7]	PCI DSS Key Requirement
27.1%	**Requirement 3 – Protect Stored Data.** Use methods such as encryption and tokenization; delete data no longer needed; track data storage, processing, and transmission; identify systems containing, and people accessing, sensitive data.
21.8%	**Requirement 6 – Develop and Maintain Secure Systems.** Perform ongoing system and application life cycle management; govern development and maintenance; use integrated change control and configuration management; establish a process to review code change logs and verify changes before releasing code into production.
30.1%	**Requirement 7 – Restrict Access by Limiting Each User's Access Rights to the Minimum.** Grant access only on a "need-to-know" basis; maintain separation of duties to mitigate insider threat activities; regularly review employee access to ensure alignment with current "need-to-know" job requirements.
31.3%	**Requirement 8 – Authenticate Access.** Authenticate access to system components; assign each user a unique identification preferably using strong MFA.
8.4%	**Requirement 10 – Track and Monitor Access.** Track and monitor access to detect and identify irregular activities and mitigate insider threat risks; ensure users are aware activities are being monitored to dissuade destructive, dishonest, illegal, and errant activities.
22.0%	**Requirement 11 – Test Security Systems and Processes.** Conduct vulnerability scanning, penetration testing, file integrity monitoring, and intrusion detection to identify and address weaknesses; when necessary, perform root cause analysis to determine cause, and preventive and detective controls to ensure that insiders aren't circumventing the control environment.
32.9%	**Requirement 12 – Security Management.** Maintain periodic training and awareness, assign clear responsibilities, and communicate policies and procedures aligned with the periodic risk assessments.

Percentage of Organizations PCI DSS Key Requirement Compliant at the Time of a Breach

[7] The effectiveness of these controls is influenced by nine factors. Read more about it in Verizon's 2018 Payment Security Report.

Victim Organizations

Certain types of data breaches correlate strongly to particular industries: attacks against point-of-sale systems in the food service industry or skimmers at gas pumps. But other kinds of attacks are more opportunistic and don't target a specific organization or industry. Privilege Misuse leans in this direction.

Some industries generate monetizable data such as bank, payment, or PII; others have customer lists or bidding information. In short, all types of companies have assets of value – and employees who could threaten these assets by misuse ranging from inappropriate web use to storing sensitive data on a thumb drive to stealing a coworker's identity.

Potential Indicator of an Insider Threat – Unreported Offers of Financial Assistance, Gifts, or Favors by a Foreign National or Stranger

Not all spies seek to be spies. Some are recruited; others divulge information unknowingly through elicitation methods. Gifts, financial assistance, or other favors from foreign nationals, businesses, or governments can compromise employees, leaving them vulnerable to blackmail, extortion, or being coerced into providing confidential proprietary information. Indications of this behavior including taking short trips to foreign countries, or visiting foreign facilities in domestic areas for unexplained reasons.

VERIS — Affected Industries

Viewing Insider and Privilege Misuse breaches over the previous year (2018), Healthcare and Social Assistance (46.4%) and Public Administration (18.5%) are the top industries involving privileged threat actors causing the most damage.

In the 2018 DBIR, a particular industry's representation in Figure 10 (below) isn't a security gauge; more doesn't correlate to less secure. The totals below are influenced by our sources: industry- or data-specific disclosure laws. The top 15 victim industries within Insider and Privilege Misuse for 2018 and for the previous five years (2014-2018) are:

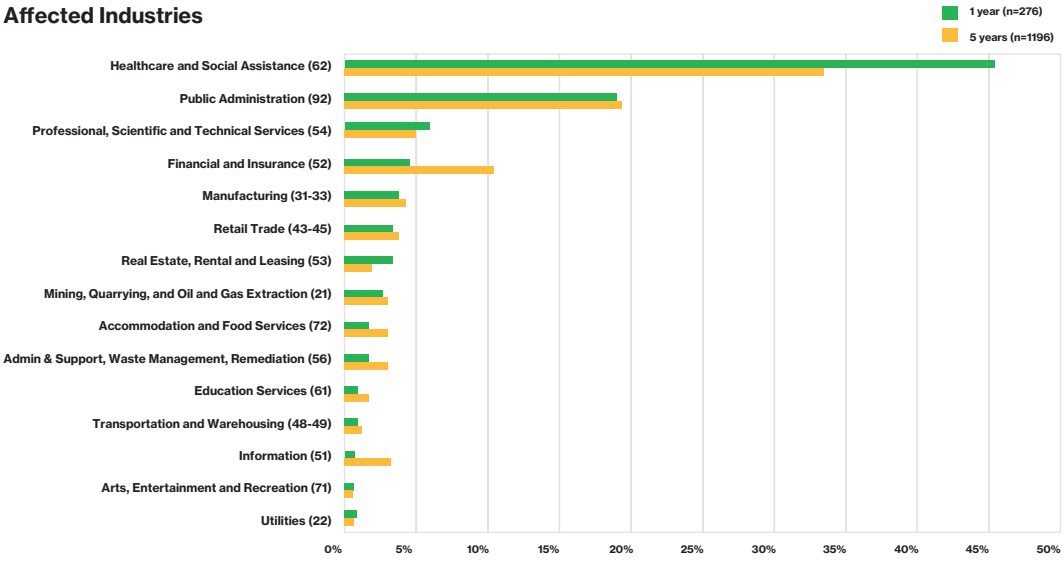


Figure 10.
Affected Industries within Insider and Privilege Misuse Breaches[8]

In both the 2018 DBIR and 2018 Protected Health Information Data Breach Report (PHIDBR),[9] healthcare is the only industry with insider actors – not external actors – responsible for a higher percentage of breaches. Easy access to medical records and personal information, combined with a duty to disclose, influences this industry's representation in Figure 10 (above).

Instead of comparing industries, it's more helpful to understand and monitor user access to sensitive data, and reduce authorization creep. We focus more on detecting potential insider misuse in the Misuse Vectors and Varieties section.

[8] NAICS = North American Industrial Classification System (www.census.gov/eos/www/naics/) or (https://www.naics.com/naics-drilldown-table/)
http://www.verizonenterprise.com/verizon-insights-lab/phi/2018/

[9] http://www.verizonenterprise.com/verizon-insights-lab/phi/2018/

Incident Response

Incident Response (IR) is the methodological approach to cybersecurity incident response. It consists of an established IR process, an IR Plan (often accompanied by specific IR playbooks), designated IR stakeholders (e.g., Chief Information Security Officer (CISO), Legal Counsel, HR), a tactical IR Team (e.g., Computer Emergency Response Team (CERT) / Computer Security Incident Response Team (CSIRT)) and a Communication Plan. The IR process usually consists of several phases such as planning and preparation, detection and validation, containment and remediation, collection and analysis, remediation and recovery, and assessment and documentation.

IR Team

Responding to and resolving cybersecurity incidents and data breaches demands effort from varied stakeholders, technical and non-technical. For insider threat situations, it's not uncommon to have HR, legal counsel, IT security, and other functional areas collaborating throughout an investigation. They address topics including scope expansion, discovering other illicit activity, sensitive data exposure (and reporting), privacy considerations, and eventual employee termination. Organizations should also contact law enforcement at the right time and with advice from legal counsel. In addition, they should engage a qualified, experienced digital forensics firm for breach response activities including deep-dive investigations as well as containment and eradication support.

IR Plan / Insider Threat Playbook

As part of an overall IR Plan, create an Insider Threat Playbook and regularly review, test and update it. It should parallel the IR Plan, but also specifically explain effective management of an insider threat data breach or cybersecurity incident. It should include guidance to involve specific stakeholders, such as legal counsel, HR, a digital forensics firm, and, if required, law enforcement. It should also include the policy on handling employee-related investigations, collecting and analyzing evidence sources, conducting witness and subject interviews and notifying organization oversight bodies, regulators, and other external entities.

Containment and Eradication

In addition to collecting and preserving any potential evidence, it's crucial to contain and eradicate any previous or ongoing threats. Threat actors may have gained physical or logical access into systems, deployed malware, destroyed hardware, modified code or even set up logic bombs for data destruction or system disruption. Containment activities include temporarily blocking outbound Internet traffic, changing user account passwords and searching for malware across the network. Eradication activities may include rebuilding affected systems, disabling compromised user accounts, and removing suspicious and malicious files and any HR-related activities.

Countermeasure – Establish Incident Management Capabilities

These capabilities can detect and respond effectively to known or suspected system breaches, system failures, or other unusual activity. These should include:

- **Incident Response (IR) Process**
  Establish a process covering the six IR phases: planning and preparation, detection and validation, containment and remediation, collection and analysis, remediation and recovery, and assessment and documentation.
- **IR Plan**
  Create an IR Plan covering the six IR phases.
- **Insider Threat Playbook**
  Create an Insider Threat Playbook for responding to insider threat cybersecurity incidents; this should supplement the IR Plan.
- **IR Team**
  Identify the IR Team; include stakeholders relevant to the specific incident; engage law enforcement when the time is right and with advice from legal counsel; engage third-party investigators when applicable.
- **Communication Plan**
  Draft an IR Stakeholder Communication Plan covering who, how, and when to contact or escalate to IR stakeholders; update regularly.

Creating an IR Stakeholder Communication Plan

Create an IR Stakeholder Communication Plan and update it at least annually and after any major security incident. Include an up-to-date IR stakeholder contact list and reporting timeframe requirements for specific stakeholders (e.g., within 24 hours, within 48 hours, within 7 business days). These timeframes should align with any existing regulatory reporting requirements.

The Communication Plan should list authorized information-sharing communication methods (e.g., email, phone, wikis, chat, as well as data- and intelligence-sharing platforms). Specifically, the Communication Plan should provide for and define emergency and secure communication methods:

- **Emergency Communication**
  Method or tool used during a cybersecurity incident to communicate critical information promptly and reliably.

- **Secure Communication**
  Method or tool used during a cybersecurity incident to communicate critical information reliably and securely (e.g., out-of-band communication, encrypted communication).

Include handling and marking requirements such as “Attorney-Client Work Product,” “Confidential,” “Privileged Communications.” Finally, prepare public relations responses for various data breach scenarios and adjust them to specific circumstances.

Digital Forensics

Digital forensics take incident responses to the next level, going deeper than Security Information and Event Monitoring (SIEM) and other tool alerts and logging. Digital forensics include evidence collection and preservation (including proper handling), evidence parsing and analysis and reporting findings.

Collection and Preservation

Scope and triage the incident quickly, but remain flexible, as the scope may need adjustment as the investigation continues. Use tested, familiar tools and procedures for evidence collection and preservation. These should include software and hardware capable of collecting physical memory dumps, volatile data, hard disk drive images, removable media images, network packet captures and NetFlow and log data. Leverage established and documented procedures for securing, preserving, collecting, storing and decommissioning evidence. Use templates, tags, chain of custody forms, and tracking logs to secure, preserve, collect and store evidence.

Parsing and Analysis

Use tested and familiar tools and procedures for parsing and analysis. At a basic level, evidence for analysis may include volatile data / physical memory, system images, malware / suspicious files, system / network logs, and NetFlow / network packets. Parse and analyze digital evidence to determine user account activity, system / network access vectors, malware execution indicators and notable files (e.g., dual-use tools, scripts, malware output files, etc.) and conduct a general security review.

Personnel Interviews

When responding to an incident, don't neglect the human element. Interview personnel with access to facilities, workspaces and digital devices. This can add insight to digital forensic findings and the overall situation. For insiders suspected of malicious activity, interviews can determine the nature of their actions. Conduct interviews under organizational policy and with HR and legal counsel involved.

Insider Threat Incident Evidence Sources

Evidence for insider threat incidents can involve any device accessed or used by the insider, or any device or person witnessing the insider's activities. These may include closed-circuit television (CCTV) footage, physical access logs, supervisor / coworker, systems / servers, smartphones / mobile devices, SIEM (e.g., network, system, Internet access, email and other application logs) logs, NetFlow data, packet captures and dark web / OSINT information.

Top Five Victim-Controllable Investigative Challenges!

In previous publications such as the DBD, we've presented the "top five victim-controllable investigative challenges." These five challenges consistently appear in our investigations and continue to plague incident response efforts. They include:

- **Logs, Logs, Logs**
  Specifically, non-existence or not enough (rolling over too quickly), or difficulty in promptly locating or retrieving.
- **Network Topologies and Asset Inventories**
  Lacking or being severely outdated.
- **Baseline Images and Trusted Processes**
  Lacking entirely, being inaccurate, or outdated.
- **"Dual-Use" Tools**
  Tools (e.g., PsExec, PowerShell) left on the system prior to its breach (storing them in the Windows Recycler isn't a security option), or with no detection of their use.
- **Self-Inflicted Anti-Forensics**
  Rebuilding systems first, then calling forensic experts; containing and eradicating but not properly documenting actions; pulling the power cable and not the network cable; and shallow investigations by unqualified IT team members.

Countermeasure – Retain Digital Forensics Services

These digital forensics services can be used for situations requiring a deep-dive investigation into cybersecurity incidents, involving collecting and analyzing network traffic, system activity, as well as data and file content activity. Services should include:

- **Digital Forensics Capability**
  Engage a qualified and experienced digital forensics firm for investigative activities including malware analysis, endpoint forensics, network forensics, threat intelligence and containment and eradication support.
- **Evidence Handling**
  Use established and documented evidence-handling procedures: evidence tags, chain of custody forms, and a tracking log to secure, preserve, collect and store evidence.
- **Endpoint Devices**
  Collect and analyze endpoint system evidence; use vetted tools and procedures for evidence collection and preservation; potential evidence includes volatile data, system images, network packet captures and log data.
- **Network Logs and Traffic**
  Collect access logs to key servers and email; collect network logs and raw network packet data wherever possible; examine quickly.
- **Other Evidence**
  Consider collecting and reviewing nonstandard evidence sources such as IT Help Desk tickets, call recordings and employee interviews.
- **Additional Support**
  Consider adding external litigation support and e-discovery capabilities if not already on board.

Scenario #3 — the Disgruntled Employee

Disgruntled employees aren't just angry. They're potentially dangerous, even if they don't resort to physical violence. Some may turn to cybercrime, including stealing information, destroying property, systems or data and disrupting business operations.

The Situation[10]

By definition, employees have access to privileged systems and information; this means large amounts of legitimate activity will need to be sorted through during breach response efforts. Any employee can be angry enough to do something malicious and therefore special care needs to be taken around events that can increase employee emotions.

Firing people was rarely an interesting job, but as I sat filling out the final forms for terminating Mr. Simpson, I breathed a sigh of relief, glad to be done with the ordeal. On the surface, it seemed like a straightforward case. Mr. Simpson's team was being merged with another team and he was unhappy with the new hierarchy. After being informed by a friend in HR about the upcoming changes, Mr. Simpson began using his administrative access to take over other accounts. He ultimately attempted to disrupt operations – a vindictive response to being underappreciated – and downloaded confidential files (a bargaining chip for his next job). It seemed so cut-and-dried – he did it and admitted to it – but still the lawyers required us to collect the evidence to prove it.

Investigative Response

I don't imagine most investigations begin with the answer, but with a very candid confession from the primary suspect, ours did. We knew how, when, and what happened from Mr. Simpson's description and by the time we engaged the VTRAC | Investigative Response Team, all we needed them to do was document and verify the claims from a technical point of view. Once we knew we had the whole truth, I could then expect to fill out a stack of forms to safely terminate Mr. Simpson's employment.

The events that led to Mr. Simpson's confession were well-documented. On an otherwise normal Friday afternoon, a programmer reported that an application was experiencing unexpected failures and an internal investigation began. This investigation turned up multiple suspicious log entries showing Mr. Simpson logging in to the application server only minutes before the problems started. The logs showed failed super user account access from Mr. Simpson, followed by password resets of service accounts. These findings could potentially have been legitimate, as Mr. Simpson was an IT administrator, but the circumstances surrounding them – no ticket or prior notification – led to the interviews in which he eventually revealed his actions, in hopes of leniency.

[10] This scenario was published originally as the DBD scenario "Disgruntled Employee – the Absolute Zero" (https://enterprise.verizon.com/resources/).

In addition to the known application server activities, Mr. Simpson admitted to accessing multiple email boxes using the service accounts to collect data for interview use and to insert scheduled jobs designed to disrupt his new team's workflows. This was a lot of data to sort through, and I honestly didn't know where to begin looking to verify these claims. Thankfully, our IT security department had called in the VTRAC Team to assist in the digital forensic examination to determine if Mr. Simpson had left any other surprises for us to find.

The VTRAC Team requested a huge number of log files and mailbox summaries, and immediately started digging in. It was only the next day when preliminary findings began coming back to us. The investigators verified that Mr. Simpson had used his access to compromise other accounts. Much to my surprise, included in their initial findings was a listing of every file he had downloaded from another user's inbox, which looked like it included everything from operations documents to product technical details. This was more than a bargaining chip. This was corporate theft. Beyond the stolen files was a second listing of scheduled jobs inserted by Mr. Simpson. The jobs were exclusively mass delete commands scheduled to occur at critical times over the next year: during tax season, prior to holiday bonuses, and a few seemingly random dates.

While our internal teams worked to remove the jobs and validate the contents of each stolen file, the VTRAC Team investigators moved on to their second phase – discovering any other activity to which Mr. Simpson may not have confessed. After requesting "network logs" from our IT security team, the investigators turned to searching for known threat actors and suspicious activity. They also focused analysis on the time range defined by the service account compromises. A few days and a dozen email requests later, a second set of findings arrived from the VTRAC Team.

The VTRAC Team review of the network traffic had identified suspicious connections to a server in Romania. This particular server was owned by a short-term lease hosting location using Bitcoin as payment. The report explained that this was currency used frequently by hackers wishing to remain anonymous, and while completely unrelated to Mr. Simpson's activity, many other attacks had involved this system. Closing out the findings was a set of instructions for our IT security team on how to find and identify the internal system in question.

It took our IT security team only a few hours to find the suspicious system and remove it from the network for further review. The on-site VTRAC Team investigators collected a forensic system image and shipped it to the VTRAC Labs for examination. This proved fruitless; comparisons with known malicious files and analysis of changes around the time of the network activity revealed nothing. Both the IT security team and VTRAC Team were baffled, as the traffic was definitely coming from this system and had stopped immediately after the device was taken offline; however, nothing seemed to be out of place. We were getting antsy.

Returning to the physical device, the VTRAC Team investigators began to collect additional forensic information and had a lucky break. While plugging in a USB keyboard to issue commands, the investigator noticed an extension on the plug itself. When pried, it popped off, revealing an off-the-shelf, clandestine keylogger. The VTRAC Team explained that the keylogger was designed to capture any input a user provided via the keyboard and was sending the capture to the rented Romanian server. I was stunned; this was the kind of thing I thought I'd see in a movie, not my job, but the proof was there in our hands.

Mr. Simpson's actions were vindictive and done in response to the recent restructuring of the company's IT Department. One of Mr. Simpson's main motivations was to make the new IT Department appear incompetent. He had admitted that he was planning to use the information he stole as leverage in finding a job with a competitor and possibly profit from his exploits. Finally, he had lied about the extent of his actions and clearly had gone beyond simply being upset. With the evidence and paperwork in hand, Mr. Simpson was summarily fired and the forensic reports were provided to law enforcement.

Lessons Learned

Our company narrowly dodged a bullet in that some of our most sensitive information and intellectual property was nearly stolen; we learned several lessons as a result of this incident. One lesson was that the friend in HR should not have notified Mr. Simpson. Details regarding restructuring and moving of specific jobs should be closely held and carefully coordinated with department managers. Another was the company should have had an action plan in place, such as increased monitoring of employees affected by the transition, to reduce the risk of vindictive behavior by those affected. Finally, as part of the transition, the company should also have conducted a thorough asset inventory. Doing so might have identified any installed keyloggers.

Misuse Varieties and Vectors

The Insider and Privilege Misuse pattern is obviously based on incidents and breaches where a threat action category of Misuse is present.

The VERIS Framework further defines actions within the Misuse category by type or variety of misuse, as well as vector of misuse. Misuse vector clarifies if privileged physical or logical access was leveraged – and if logical, whether the activity was conducted from a cubicle, corporate LAN, or via remote access. This section will address these issues, then look deeper into specific misuses.

Countermeasure – Employ Physical Security Measures

Employ physical security measures to limit access to sensitive areas. This should include identity badges, turnstiles, gates or doors with card swipes, and PIN Entry Device or biometry readers for multi-factor authentication (MFA). For highly sensitive areas, restrict cameras, smartphones, and external storage devices; restrict Bluetooth and Wi-Fi; and conduct monitoring and logging.

Monitor and set alerts for suspicious physical access patterns and activities for sensitive areas. Use physical security measures such as cameras, motion detectors and guards at entrance and exit points.

VERIS — Misuse Varieties

When we examine misuse varieties in last year's 2018, we see Privilege Abuse (73.6%), Data Mishandling (20.1%), and Possession Abuse (8.1%) as the top misuse varieties. The top 10 misuse varieties within Insider and Privilege Misuse for 2018 and for the previous five years (2014-2018) are:

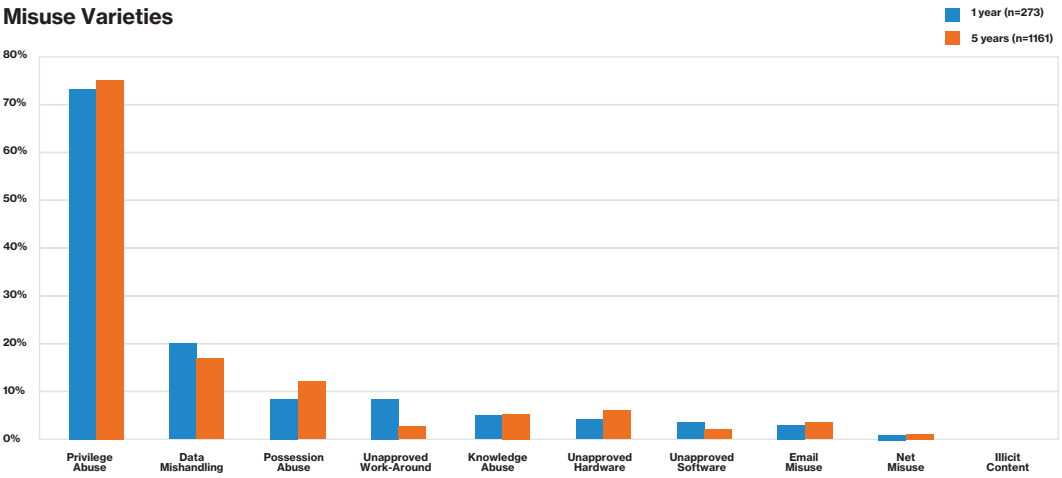


Figure 11.
Top 10 Misuse Varieties within Insider and Privilege Misuse Breaches

Privilege Abuse is simply using existing logical access in an unauthorized manner. An example is a bank employee accessing a customer's account and writing down their account numbers. Its simplicity and the many employee roles requiring swift access to sensitive data are the main reasons for its prominence. Examples of Data Mishandling are copying sensitive information to a USB flash drive or emailing data to personal email accounts to work over the weekend (or something more sinister).

Possession Abuse is similar to Privilege Abuse, only this is leveraging physical access to data and assets. Historically we have seen incidents where food servers will use a hand-held card skimmer while they have a customer's physical payment card. Other misuse actions include leveraging private knowledge and breaking various use policies.

VERIS — Misuse Vectors

When we survey misuse vectors within Insider and Privilege Misuse in last year's DBIR, we see LAN Access (82.5%) and, distantly in second place, Physical Access (13.4%) as the top misuse vectors. This correlates with Privilege Abuse and Possession Abuse threat actions in the previous section. Most unsanctioned activity is within the cubicle walls during employee shifts:

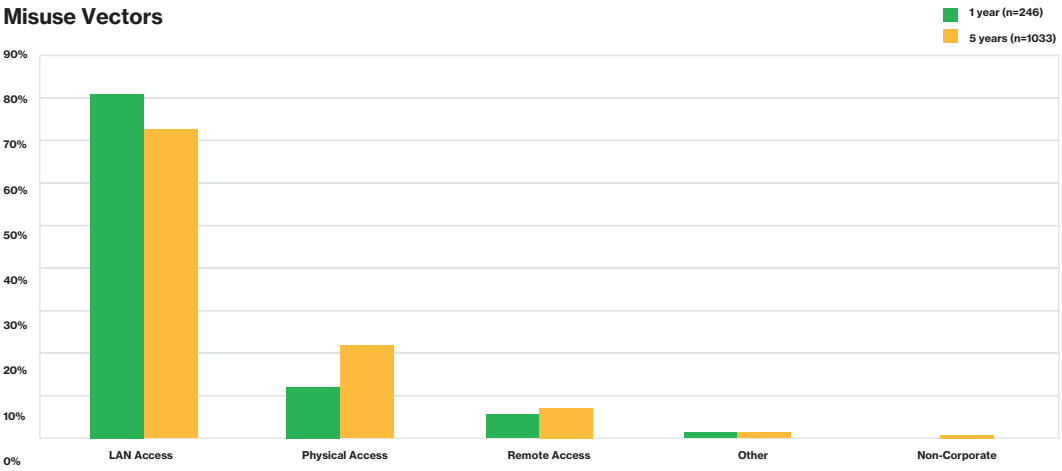


Figure 12.
Misuse Vectors within Insider and Privilege Misuse Breaches

Remote access entry points shouldn't be ignored. We encounter cases where insiders will use local and remote connectivity in their actions. There are also numerous instances of recently dismissed employees using old remote access privileges (that should have been disabled) to log in to an organization's environment. This is categorized as Privilege Misuse, since from a VPN server viewpoint, the privileges still exist.

Implementing Multi-Factor Authentication

MFA is access control authenticating users with two or more independent forms of identification. These span three categories: something you know, such as a user-created password, something you have, such as a one-time passcode (OTP), and something you are, such as your fingerprint or retina scan.

If your organization hasn't already done so, move beyond single-factor authentication and implement MFA. Require MFA for VPN remote connections to the corporate environment, and especially for accessing sensitive resources such as VPN or email from external sources.

Identity and Access Management

An effective Identity and Access Management (IAM) Framework includes core processes, supporting processes and is governed by stated policies. Core IAM processes include:

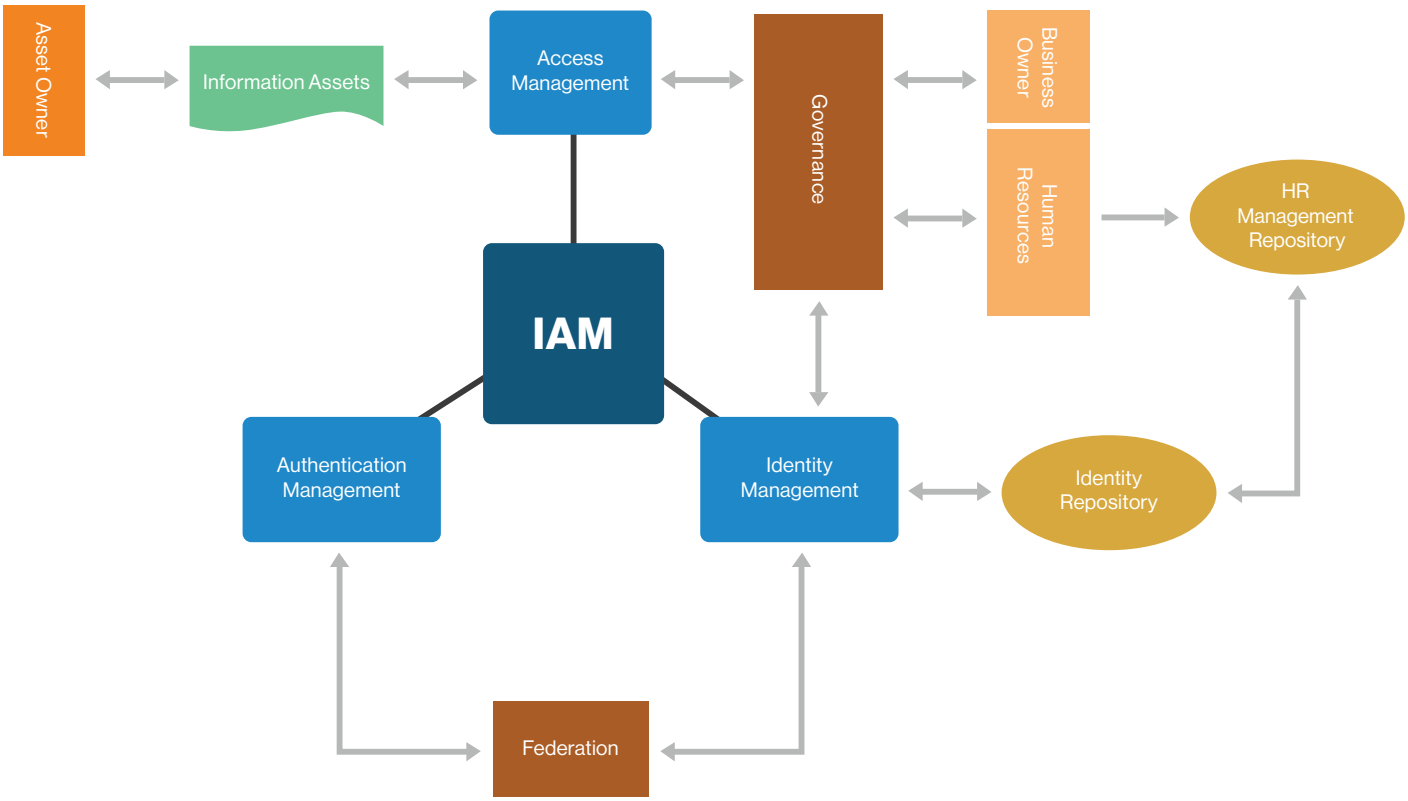


Figure 13.
IAM Framework

Identity Management

The primary goal of identity management is to address the life cycle of identities for objects, entities (e.g., systems, devices, or other processes), and persons needing trusted access to organizational assets (e.g., information, systems, servers, networks and facilities). Accordingly, identity life cycle management must include creating, provisioning, updating, tracking and ultimately decommissioning identities.

Federation

In the IAM Framework in Figure 13 (p. 47), federation is between identity management and authentication management. Identity federation adds a new dimension to authentication management, by connecting multiple identity management systems. It's often used for accessing cloud-based applications, or by organizations using multiple identity repositories. Identity federation adds concepts of "trust" among connected identity systems. User credentials are stored at their home organization, commonly called Identity Provider.

A Cloud Access Security Broker (CASB) solution enforces security policy between an enterprise and a cloud service provider. Logging on to a cloud service or an application handled by another identity management service provider, requires this service provider to trust another provider to validate the user's credentials. Identity federation is often used in Single Sign-On (SSO) schemes. SSO can be accomplished using identity federation. However, the opposite isn't necessarily true.

Authentication Management

The primary goal of authentication management is to link a person who wants to use an application or system (component) to a digital identity, establishing the validity of this digital identity. By itself, authentication doesn't authorize the identity to use the application or system (component). Methods for authentication include:

- Traditional verification using a single verifier (something you know, such as a username-password combination).
- Biometric (physical trait) authentication using a single verifier (something you are, such as a fingerprint).
- MFA using a secondary verifier (something you know complemented by something you have or something you are).
- SSO through a centralized authentication system.

These can be used for multiple forms of access: specific (mobile) devices, remote access, or direct access.

Access Management

The primary goal of access management is to approve and assign access privileges, manage changes, and monitor the access environment. This ensures alignment with business requirements, and helps reduce risk to organizational assets. The goal is accomplished by defining access controls and constraints, based on a model sanctioned by information asset owners.

Governance

In the IAM Framework in Figure 13 (p. 47), governance falls between identity management and access management. Periodic reviews of identities and associated access logs are essential to find and quickly correct inconsistencies in access privileges and identity definitions.

Protecting Privileged Accounts

Taking these steps can help protect privileged accounts:

- Minimize privileged accounts; remove accounts and account privileges when no longer required.
- Monitor sessions; periodically audit accounts and account privileges.
- Make it policy and practice to use admin accounts (with MFA) only when needed; use user accounts for everyday functions.
- Implement least privilege access control; limit access to only those required to perform the task.
- Implement MFA; use strong passwords; protect credentials through vaulting with automated rotation.
- Manage shared privileged accounts through user request and approval workflows.

Countermeasure – Employ Identity and Access Management Measures

Employ access measures to manage identity, access, and authentication into the enterprise environment. These should include:

- **Identity Management**
  Address the life cycle of identities for objects, entities (e.g., systems, devices, or other processes) and persons needing trusted access to organizational assets.

- **Authentication Management**
  Link a person who wants to use an application or system (component) to a digital identity, establishing the validity of this digital identity.

- **Authentication Management**
  Approve and assign access privileges, manage changes and monitor the access environment.

Consider using a PAM (Privileged Access Management) solution, adding protection for privileged access, which incorporates privileged user logon with login channels, authentication options, password vaulting, session management, host access control with privilege escalation and logging throughout the process.

Privilege Access Management

Special consideration should be given to accounts with administrative privileges. Typically, these admin user accounts are granted elevated privileges for managing IT infrastructure services and components. Examples of accounts with administrative privileges are Windows domain admin accounts, accounts for systems and network engineering, non-personal, functional, or shared accounts such as "root" or "DBA," and service accounts.

Privileged accounts are those granted privileges beyond everyday user accounts. Having access to privileged accounts provides a threat actor (or legitimate user) with access to additional systems and services. These are often among the first targets of external attackers or malicious insiders intending to cause financial loss, data loss and reputational damage.

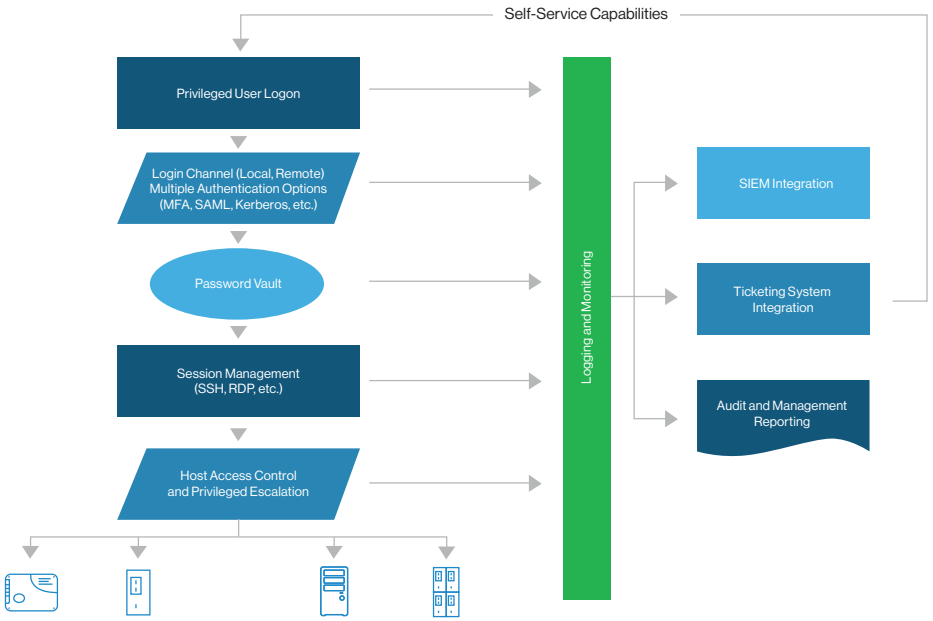
Privileged accounts can be human-used or non-human-used. Human-used privileged accounts are typically personal accounts to which elevated privileges have been assigned (e.g., domain admin), or non-personal shared accounts used for system management (e.g., "root" or "DBA"). Non-human privileged accounts are typically service and application accounts. Common privileged accounts are:

Account Type	Characteristics
Shared Administrative Accounts	Shared privileged non-human accounts providing admin access to a local host (e.g., root).
Privileged Accounts	Privileged user accounts providing admin access to one or more systems.
Administrative Accounts	High-privileged user accounts with administrative access to systems and servers within a domain; having complete control over all domain controllers and the ability to modify privileged account membership within the domain.
Emergency Privileged Accounts	High-privileged user accounts providing unprivileged users with administrative access for securing systems if an emergency occurs (a.k.a. breakglass or firecall accounts).
Service Accounts	Privileged non-human local or domain accounts used by applications or services to interact with the operating system.
Accounts	Privileged non-human accounts used by applications accessing databases running scripts or sub-processes and accessing other applications.

Table 14.
Common Privileged Accounts

A Privileged Access Management (PAM) solution is the first line of defense for protecting infrastructural components (e.g., network components, databases, configurations for systems and applications) in an IT landscape. PAM aims to mitigate threats to accounts that hold privileges beyond those required for regular users performing daily work functions.

Given that PAM is a high-tech, not out-of-the-box solution, it requires integration into overall IT security architecture. A high-level PAM solution is outlined in Figure 14A (below):



Access Flow	Mapped Solutions
Privileged User Logon + Login Channels	Secure logon (e.g., local, remote) capabilities.
Authentication Options	Authentication capabilities (e.g., MFA, SAML, Kerberos).
Password Vaulting	Check-out / check-in credentials with automated rotation capabilities.
Session Management	Enable session management and recording capabilities.
Host Access Control + Privilege Escalation	Manage shared / personal privileged accounts.

Figure 14A.
PAM Solution Capabilities

Potential Indicator of an Insider Threat –
Attempts to Gain, or Actually Gaining, Access to Systems or Data
Without a Valid "Need-to-Know"

Inside threats can be difficult to defend against because they often know how to subvert detection systems. They can misuse servers and systems to gain access to unauthorized information such as trade secrets, proprietary information and sensitive technology.

A malicious insider can authorize applications to transfer money or send trade secrets, or steal payment information by bypassing usual security authentication and authorization steps. Gaining access, they can disclose sensitive information resulting in loss of reputation, market share and competitive edge.

Warning signs for these individuals include:

- Asking others for access to sensitive information they're not authorized to access.
- Attempts to remotely access a computer network from outside systems without proper authorization.
- Unauthorized removal of sensitive material from the workplace.
- Bringing sensitive information or systems home or on trips without proper authorization.
- Working unusual hours, or accessing IT systems and areas after normal hours without logical reason.
- Bringing cameras or other recording devices without approval into areas with sensitive material.

Scenario #4 — the Malicious Insider

Malicious insiders who hide their true feelings can be difficult to detect. They typically act on their own, stealing information for personal gain. Leveraging inside knowledge and access, they are often tougher to defend against than outsider attacks.

They leverage access to endpoint systems, servers, networks, and organization domains – often using access given to them to perform their daily duties. Because they're inside the system, there's no need to hack into the enterprise or navigate its defenses.

A malicious insider is a current or former employee, contractor, or business partner who meets these criteria: they have or once had authorized access to an organization's network, system, or data; and they have intentionally exceeded or intentionally used that access to negatively affect the organization's information.

The Situation

"Snap. Snap. Snap." The sound is coming from a coworker's cubicle: a mobile phone taking photos. Maybe they're selfies? The noise keeps repeating, so you overcome social inhibitions and check what's happening.

Your coworker is taking pictures of their computer screen – which is showing customer financial data. You tell your manager, who confronts your coworker immediately. They claim they were just taking selfies. Should management take their phone? What if it's a corporate phone?

Investigative Response

Don't take the phone. Instead, call a rigorous forensics investigations partner such as Verizon and ask them to pull photos from the employee's corporate cloud drive. In this case, management uncovered hundreds of photos of customer banking data. The employee had been doing this for weeks, according to time stamps.

What would you have done if this was their personal phone?

During the exit briefing, the employee signs papers claiming it's all a misunderstanding. They wouldn't have done anything with the data, and it's not technically a breach of information since the photos never left a corporate device. They went from corporate monitor to corporate smartphone, and they will sue you for wrongful termination.

You engage the VTRAC | Dark Web Threat Hunting Team to see what they can find on the surface, deep, and dark web. They quickly find the coworker's partner on social media, and that they have a criminal record for putting card skimmers at gas pumps and selling the information on the dark web.

Your investigation also uncovers that another employee seated nearby also witnessed suspicious behavior (they never reported it; another problem). This employee had been using headphones and didn't hear any phone camera shutter noise.

You're still not done. Affected customers could potentially fall victim to financial fraud. You need to know whether the employee accessed other records: maybe copied by hand, on another phone, or transmitted by other means. How far back do you take response effort? Does this qualify as a breach? Do you report this to law enforcement? What policy should you implement to prevent this from happening again?

Lessons Learned

In this case, the malicious insider was stealing customer data for personal gain. Other insiders may steal, destroy, or release sensitive information for revenge or other motives. To do so, they may leverage their own privileges or steal coworkers' credentials to gain unauthorized access. Key countermeasures to prevent future malicious insider activities include:

Mitigation and Prevention

- Control and restrict data access to sensitive information through the principle of "need-to-know."
- Increase monitoring and logging of sensitive and restricted areas, systems and data.
- Monitor users to include external storage devices; restrict camera and smartphone use in sensitive areas.
- Disable access for activity deemed inappropriate or posing organizational risks.

Mobile Device Security –
IT Best Practices

Increased mobility and improving technology mean even more data is communicated via smartphones. Rules and policies may prevent this data from being compromised:

- Use a Mobile Device Management (MDM) console to establish centralized rules and policy enforcement on corporate-issued and BYOD items.
- Require users to enable screen locking with eight or more uppercase-lowercase-alphanumeric-special characters passcodes on devices accessing organization information.
- When storing, transmitting, or processing sensitive information, enable encryption features for data at-rest and data in-motion.
- Perform security audits on all authorized mobile device apps.
- Establish a dialogue with users to prevent unauthorized work-arounds to security methods.

Maintain awareness on mobile security. Monitor for new threats and educate users to stay ahead of adversaries.

**Mobile Device Security –
User Best Practices**

Mobile devices are a necessity in our lives – but they're also targets. These suggestions may reduce the risk of mobile devices being compromised:

- Always use a password. Passcodes with eight or more uppercase-lowercase-alphanumeric-special characters are more secure than the standard 4- or 6-digit PIN codes.
- Never leave a device unattended! Physical access to a mobile device is the easiest way to gain unauthorized access.
- Keep the device up to date to avoid common methods of mobile breaches.
- Only use trusted sources for apps. This includes the iTunes store for Apple devices, and Google Play for Androids. Downloading third-party apps from other sources can enable malicious software.
- Use EDR solution to identify affected systems. Once an affected system is identified, disk forensics paired with an EDR solution can allow a direct view into additional systems that may be affected.
- Enable screen locking. Shorter intervals between use and auto lock reduce chances for others to gain easy access.
- Avoid jailbroken devices, which have decreased security.

**Potential Indicator of an Insider Threat –
the Disgruntled Employee**

Insider threat activity is an abuse of authorized access to any organizational, industrial, or government resource by an individual who harms the interested party. Disgruntled employees can compromise information or systems – and be exploited by malicious entities for information or system access. Potential causes and indicators include:

- Employees disgruntled with an organization, supervisor, or coworkers strong enough to cause them to seek revenge.
- Attempts to encourage others to violate laws or disobey organizational security policies.

Assets and Data

As we've seen, threat actor categories include various motivations such as Financial, Fun, or Espionage. The VERIS Framework breaks down these tangibles into affected asset varieties and data varieties.

VERIS — Affected Assets

When we examine affected asset varieties within Insider and Privilege Misuse over the previous five DBIRs (2014-2018), Server (69.6%), Media (13.8%), User Device (12.5%), and Person (11.2%) are the top affected assets:

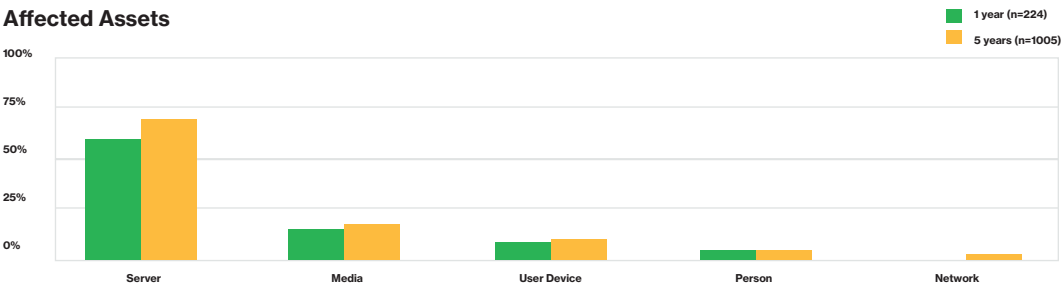


Figure 15.
Affected Asset Varieties within Insider and Privilege Misuse Breaches

Servers are the most common assets affected; these are predominantly databases that internal actors access with existing privileges, but in an unauthorized manner. The oft-cited example of healthcare workers accessing medical records for identity theft or satisfying curiosity is a common scenario. Public sector and financial organizations are also prevalent in this style of attack.

The Media asset category is typically employees misusing physical access to obtain corporate documents or customer payment cards.

General privilege abuse of desktops and laptops is the typical action taken against User Devices, but use of unapproved hardware (e.g., USB flash drives to exfiltrate data) and data mishandling (e.g., emailing data to personal accounts) are also present.

The Person category includes situations where human behavior is influenced to act in an inappropriate or malicious manner. In over 60% of breaches involving human assets, bribery or solicitation was recorded.

Countermeasure – Perform Vulnerability Scanning and Penetration Testing

Vulnerability assessment and penetration testing activities can help identify gaps within a security strategy, including potential ways for insider threats to maneuver within the enterprise environment. Effective assessments should include:

- **Vulnerability Scanning**
  Mainly automated, conducted at least quarterly, and performed by internal and external teams; scanning seeks vulnerabilities in the network (and/or applications) and associated exploit vectors.

- **Penetration Testing**
  Mostly manual, conducted annually, and typically performed by an external team; an exploit-related vulnerability assessment; penetration tests seek to leverage exploits from identified vulnerabilities to access the network and applications.

- **“Red Team” Penetration Testing**
  An advanced penetration test; mainly manual, conducted as required, and performed by an external team, which takes the role of a threat actor to test a security strategy and identify gaps.

- **“Purple Team” Exercises**
  An advanced penetration test; matches “Blue Team” (organization) with “Red Team” (attackers) in a coordinated, learning effort.

Asset Management

Knowing the data an organization keeps and where it's stored is essential to effective mitigation and response. To protect data and investigate its potential compromise, maintain an up-to-date asset inventory, track assets, and know where sensitive data is.

This means conducting periodic asset inventories and e-discovery exercises. Keep employee-assigned systems and data storage devices for a predetermined time after employee departure from the organization. Monitor current systems for data loss. If external media devices are authorized, monitor and log data transfers. Scan for sensitive data improperly marked or stored in unauthorized locations.

Use an IDS / IPS. When possible, leverage an FIM solution and whitelist applications. FIM validates the integrity of operating system and application software files, using a verification comparison between the file state and the known, good baseline. By using a FIM solution, data changes can be detected and alerted. Limit unauthorized or BYOD access by disabling automatic network configuration, such as Dynamic Host Configuration Protocol (DHCP).

Countermeasure – Employ Endpoint Security Solutions

Solutions for endpoint activity monitoring, collection, and analysis should include:

- **Host-Based Firewalls**
  Software or hardware security system for monitoring and controlling incoming and outgoing network traffic based on predetermined security rules.
- **Host IDS**
  System for analyzing packets and alerts (passive) on suspicious host activity.
- **Host IPS**
  System for analyzing packets and blocking (active) suspicious host activity; typically possesses a subset of IDS rules and coexists with IDS.

Countermeasure – Employ Endpoint Security Solutions (continued)

- **EDR Solution**
  Software solution for attack monitoring; auditing and logging; evidence collection and incident response.
- **Asset Inventory**
  Tool for tracking all assets, including critical servers and systems.
- **Critical Assets**
  Identify, track, and account for critical assets; prioritize them for enhanced protection and monitoring.
- **System Baselining**
  Solution for establishing system-hardening baselines; deriving known applications and trusted processes for monitoring and investigative purposes.
- **Removable Media Policy**
  Requirement for eliminating or restricting USB flash drive and other removable media usage.
- **Anti-Virus (AV) Protection**
  Solution for protecting systems from viruses.
- **Network and Application Logs**
  Reviewing logs for suspicious, anomalous system activity.
- **Device Encryption**
  Consider encrypting hard disk drives and mobile systems including laptops, smartphones, and portable storage devices.
- **SIEM Solution**
  Tool for reviewing aggregated log data from network, security devices, systems, and applications for suspicious or anomalous system activity.
- **FIM Solution**
  Tool for monitoring and validating file integrity and system changes.
- **Application Whitelisting (AWL)**
  Solution for controlling applications permitted for installation, as well as execution on an endpoint.
- **Configuration Management / Patching Management**
  Solutions for managing system configuration changes and application patching updates.

Monitor suspicious system activity, with alerts for unusual off-hours activity, volumes of outbound activity, and remote connections. Leverage an SIEM capability to monitor insider threat activities; periodically update detection rules and watch lists.

VERIS — Data Varieties

Data Varieties represent the type of information targeted, such as Personal, Secrets, or Source Code. Examining Insider and Privilege Misuse over the previous year (2018), we see Medical (44.9%), Personal (32.1%), and Internal (14.8%) as the leading types. The top 10 Data Varieties within Insider and Privilege Misuse for 2018 and the previous five years (2014-2018) are:

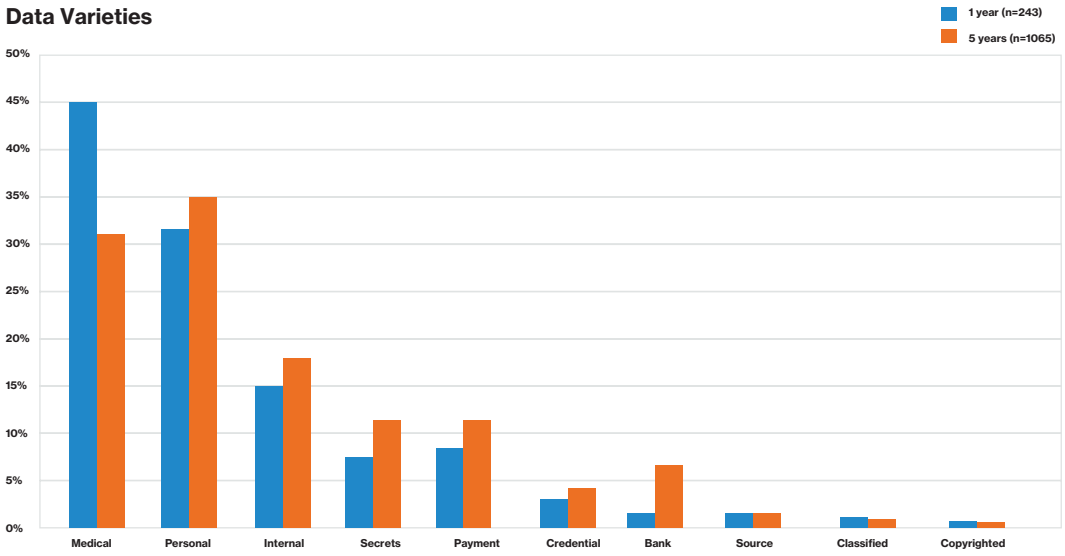


Figure 16.
Top 10 Data Varieties within Insider and Privilege Misuse Breaches

As expected, the Healthcare industry represents the majority of victims experiencing medical data breaches (84%). Healthcare is also one of the most common industries (with the public sector) in personal data breaches. Recalling "Figure 10. Affected Industries within Insider and Privilege Misuse Breaches," Healthcare and the public sector comprised the top two industries. Clearly, there is a significant association between the top industries and top compromised data varieties. As previously noted, this is influenced by our data contributors, as well as by industry-specific notification laws.

VERIS — Sensitive Data Breached by Industry

When we examine the combination of sensitive internal data (Internal), intellectual property (Secrets), and classified information for the previous five DBIRs (2014-2018), we see vast diversity in industry representation:

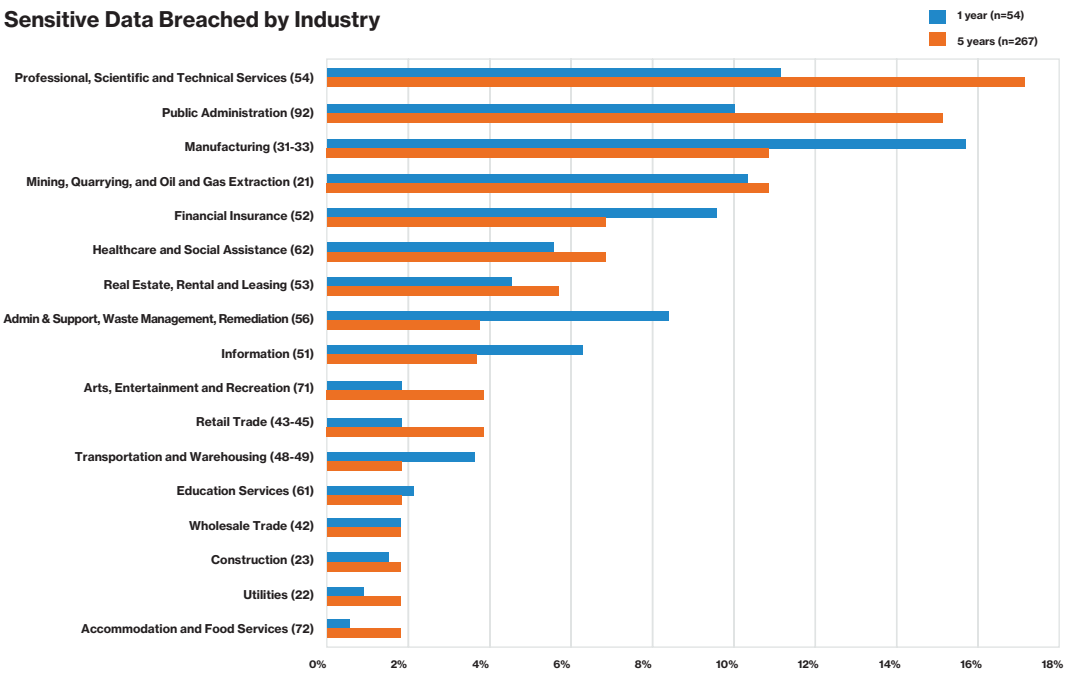


Figure 17.
Industries within Insider and Privilege Misuse Breaches Involving Select Data Varieties

When we focus on data varieties that aren't as monetizable as payment card or banking information, industries such as Manufacturing, Mining and Professional Services become more prominent.

Industries have varied threat landscapes, with some more susceptible to insider threats than others. Much of this is driven by actor motives and the data types insiders can access. Threat modeling should reflect where data resides or is processed within a specific organization, and how its employees and partners could potentially misuse it.

Data Classification and Protection

Simply put, data needs protection from unauthorized access; this is especially true for sensitive data. And ultimately, this data has to be protected from both inside and external threat actors. Components of a data protection solution should include data classification and data protection, at least.

Classification

As data is created, it's essential to classify it correctly. In turn, classification determines who should have access and what they can do with the data. Data creation typically occurs in two ways: automated or manual.

Automated
Examples include data downloaded to or uploaded from a specific application, or data written by a specific application to a well-defined storage area. It could involve sensitive information downloaded from a back-end server. The location of the download isn't a reliable way to determine data sensitivity; in the case of a back-end server, classification at the point of creation (i.e., when the information is downloaded) is needed since the data could be stored anywhere.

Manual
Users often manually create sensitive information, such as intellectual property. This can be done through email or another client application. Users must be able to classify manual information in a uniform and persistent manner (i.e., more than just a text string at the bottom of a presentation).

Accurate classification is the basis for a successful data protection program. Additionally, classification must be meaningful – if data is classified as sensitive, that should come with a clear definition and protection policies. Data classification should also be visible to users, together with displays about classification policies, for a powerful learning experience.

Protection

Instead of only blocking potential intrusions, protecting data (such as by encryption) is an important approach, and also helps employees carry out daily tasks more seamlessly. Data protection should be based on a data classification policy and be uniform throughout the organization. Encryption mechanisms that can't be inspected by the organization must be prevented.

Complement data classification with a content protection solution, provide persistent encryption capabilities, link to classification policies, and automatically invoke these when assigning classification levels.

Hardening the Digital Environment

Hardening the digital environment includes tightening up the security of the network, systems, applications, data, and accounts:

- **Network**
  Segment the network and restrict access to sensitive systems; place firewalls on the outer perimeter and between internal segments; encrypt external access and Wi-Fi traffic.
- **Systems**
  Encrypt hard disk drives and mobile systems such as laptops, smartphones, and portable storage devices; eliminate or restrict the use of USB flash drives and other removable media; ensure each system has a host-based AV solution and firewall installed.
- **Applications**
  Uninstall unneeded apps; apply patches promptly; disable any auto-run features; ensure AV is running and virus definitions are up to date.
- **Data**
  Regularly remove unneeded data from servers and shares; back up critical data and test these periodically; use a DLP solution to detect unauthorized movement of sensitive data.
- **Accounts**
  Establish a robust password policy; use MFA for remote and cross-segment access; prohibit shared accounts; remove local admin rights and disable unnecessary accounts; monitor admin and service accounts.

Countermeasure – Apply Data Security Measures

Managing the data management life cycle while maintaining confidentiality, integrity, and availability, by including:

- **Data Ownership**
  Identifying data owners for data classification.
- **Data Classification**
  Classifying data for determining access and protection measures.
- **Data Protection**
  Protecting data through endpoint security solutions (e.g., system baselining, AV protection).
- **Data Disposal**
  Properly disposing data at the end of its life cycle.

Scenario #5 — the Feckless Third-Party

The feckless third-party is defined as a threat actor with inside access who through negligence, misuse or malicious intent compromises organizational security.

The Situation[11]

While many investigations at the VTRAC | Labs are straightforward, involving commodity servers and operating systems, others require working directly with embedded systems or hardware components. Such engagements are sent directly to the Labs, where we have sophisticated tools – beyond what a typical investigator can deploy on the go.

In one investigation involving suspected cyber-espionage, a customer contacted us to determine why certain devices were behaving suspiciously. Reviewing network traffic, the customer realized a particular server model they used extensively had been sending Simple Network Management Protocol (SNMP) traffic to a Southeast Asia IP address. Since this IP address wasn't associated with any of their vendors or customers, they were concerned about data exfiltration. This was amplified when the server vendor couldn't explain the remote IP address connections.

Investigative Response

The customer provided a physical server, a verified forensic image of another server, and the suspicious remote IP address. We went to work, setting up an air-gapped environment to test the server and physically inspecting its components.

Nothing out of the ordinary was discovered during the physical inspection; however, a remote management module, which is the system component responsible for communications management, was identified.

Next, we recreated the suspect communication. The server was connected to a full packet capture (PCAP) device. On booting, it attempted to find the network node associated with internal (RFC 1918) IP 172.16.x.x. Assuming this was its default gateway, the server was powered down. Traffic for IP 172.16.x.x was routed to the network PCAP device, and the server was rebooted. Once the server received IP 172.16.x.x in response, it attempted to communicate with the suspicious IP address.

These communications were controlled by the server's firmware, so our next step was to review this firmware. We downloaded several versions of the firmware from the vendor's website. A review determined the boot loader and file system in use. We found no indication of the suspicious remote IP address hard coded in the firmware.

[11] This scenario was published originally as standalone DBD scenario "Supply-Chain Reaction – the Whole Enchilada" (https://enterprise.verizon.com/resources/).

With the software ruled out, we used an oscilloscope to determine the location and specifications of an active serial port for debugging. This debugging port offered a way of connecting to the main processor associated with remote management. This permitted monitoring of the management card boot process and access to its command shell.

We extracted the firmware source code from the server for analysis, including searching for the suspicious IP address. It took effort, but we eventually found the suspicious IP address in hexadecimal format within a configuration file. This configuration file was identical to the ones downloaded, but contained the suspicious IP address in encoded format.

Ultimately, it was determined that all system components and code matched those shipped from the vendor. Due to the complexity of modern computing environments and corporate networks, it's a challenge to keep track of every server and connection required for operation. Here, even the vendor was unaware of owning and using this suspicious IP address, which itself led to a very lengthy investigation. Rogue mechanisms, such as remote management modules or similar embedded devices, can provide entrance and exit vectors for threat actors – and must be addressed by security measures.

Lessons Learned

The customer had several good security practices in place. For instance, their detection of the unexpected traffic resulted from routine network monitoring. However, had they tested the systems prior to deployment, they might have noticed the suspicious traffic and evaluated the risks. This would have also offered them an opportunity to work with the vendor at a more relaxed pace.

It's good practice to upgrade to the latest version of firmware for testing prior to deployment. With the new firmware in place, a baseline of system behavior should know what "normal" looks like. Familiarity with normal setup and behavior can be the difference between detecting anomalies signaling an attack and becoming aware at a far less convenient time.

Mitigation and Prevention

- Vet hardware supply chains, to include original equipment manufacturers and value-added resellers, for reputation and reliability.
- Adopt an IT management process that covers design, testing, management and review that aims to ensure confidentiality, integrity, and availability.
- Maintain an asset inventory; track and account for all assets, to include critical servers and systems.

Detection and Response

- Monitor for suspicious network traffic, such as unusual off-hours activity, volumes of outbound activity, and remote connections.
- Keep baseline system images and trusted process lists; use these known standards to compare with compromised systems.
- Temporarily block outbound Internet traffic, change user account passwords, and search for indicators of compromise.
- Disable compromised user accounts, remove malicious files, rebuild affected systems.

Potential Indicators of Insider Threat Activity

While investigating various cybersecurity incidents over the years, we've seen various indicators of potential insider threat activity. Some of these include:

- Attempts or successful access to systems and data without a valid "need-to-know."
- Requesting access to information outside of normal job duties.
- Unusual or erratic personal behavior.
- Highly disgruntled attitude.
- Working odd or late hours without reason.
- Apparent, unexplained affluence or excessive indebtedness.
- Efforts to conceal foreign contacts, travel, interests, or suspicious activity.
- Unreported offers of financial assistance, gifts or favors by a foreign national.
- Exploitable behavior, such as criminal activity, sexual misconduct, excessive gambling, alcohol or drug abuse, or problems at work.

We denote these as possible indicators, because taken individually or even in twos and threes, they don't necessarily mean an insider is conducting malicious activity. But taken as a whole, they may be concerning, and attention should be paid.

Final Thoughts

As this report makes clear, while the insider threat may be complex and challenging, it's not impossible to defend against.

Ultimately, when implementing an insider threat strategy, focus on two factors: assets and people. Know your assets: what and where are the most important ones, both static and kinetic, and how you'll protect, monitor, and investigate their compromise. Know your people: who has access to assets, and how you'll vet, monitor, and investigate any potential malicious activities.

Focus on protecting your high-value assets, both physical and kinetic, then address areas of highest risk. By addressing the most impactful situations, rather than just applying blanket coverage, you can improve your Insider Threat Program's effectiveness. These 11 countermeasures can reduce risks and assist in incident response:

1. Integrate Security Strategies and Policies
2. Conduct Threat Hunting Activities
3. Perform Vulnerability Scanning and Penetration Testing
4. Implement Personnel Security Measures
5. Employ Physical Security Measures
6. Implement Network Security Solutions
7. Employ Endpoint Security Solutions
8. Apply Data Security Measures
9. Employ Identity and Access Management Measures
10. Establish Incident Management Capabilities
11. Retain Digital Forensics Services

ISO 27001, the NIST Cyber Security Framework (CSF), and other compliance programs and guidance frameworks can help you implement these countermeasures. Ultimately, you have the power and information to minimize your risk of becoming the subject of the next cybercrime headlines.

verizonenterprise.com