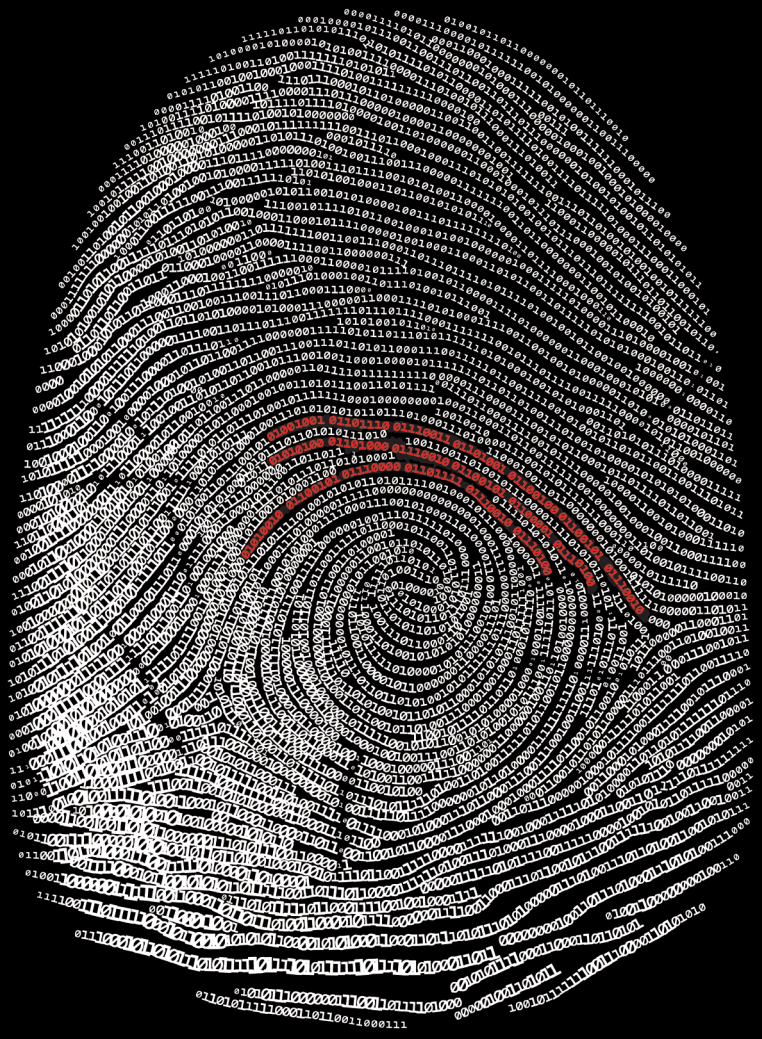
Insider Threat Report

Executive Summary



verizon
business ready

The Verizon Data Breach Investigations Report team now brings you The Insider Threat Report.

This comprehensive examination of internal threats facing organizations of all kinds has actionable, data-driven insights for CISOs and business leaders alike. Learn how rogue partners, careless contractors and negligent (or malicious) employees can seriously disrupt your organization – with significant financial and legal ramifications.

As much as you may enjoy working with many of your colleagues, some of their behaviors may put your organization's sensitive data at risk.

Verizon's new Insider Threat Report (complimentary for all) draws on lessons learned from hundreds of data breach investigations by Verizon's world-renowned digital forensics team. It also features new data and insight from industry groups and partners, as well as the 2018 Verizon Data Breach Investigations Report (DBIR). The Insider Threat Report:

- Situates insider threats within the context of overall cyber threats, illustrating the risks to your organization's vital assets.
- Identifies varied internal threat actors, outlining their motivations and methods to help you defend against them
  .
- Takes a deep dive into the risks and potential abuses associated with privileged access
- Includes case studies from the recent Verizon Data Breach Digest to show how insider threats unfold.
- Offers practical advice on implementing policies and controls to mitigate insider threats.

In outlining measures for an Insider Threat Program, we start with two perspectives: knowing your assets, and knowing your people (including their access to assets). This knowledge then informs 11 distinct approaches to reducing insider threat risks and improving response capabilities.

Verizon's Insider Threat Report has insights for everyone from IT professionals to security executives to non-IT business leaders who may not completely grasp potentially devastating threats from within the organization.

Full Speed Ahead: Fewer Speed Bumps for Internal Bad Actors

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.

The time from an unsanctioned action (such 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:

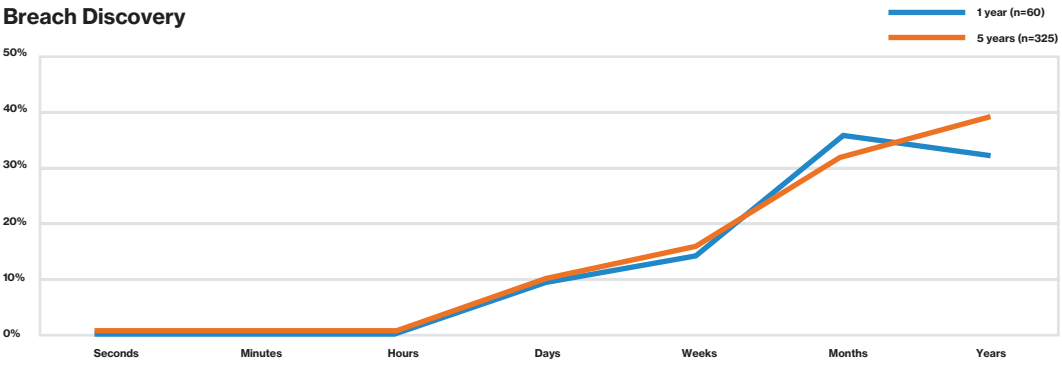


Figure 3.
Breach Time to Discovery within Insider and Privilege Misuse Breaches

Click! That's the sound of a mobile phone taking photos coming from a coworker's cubicle. Maybe they're just taking selfies. But the sound is repeating, so you overcome social inhibitions and check on what's happening.

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

The Insider Threat Report takes you through best practices for responding to this scenario – and others that occur more often than many think.

No Industry is Immune—Especially the Sensitive Ones.

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:

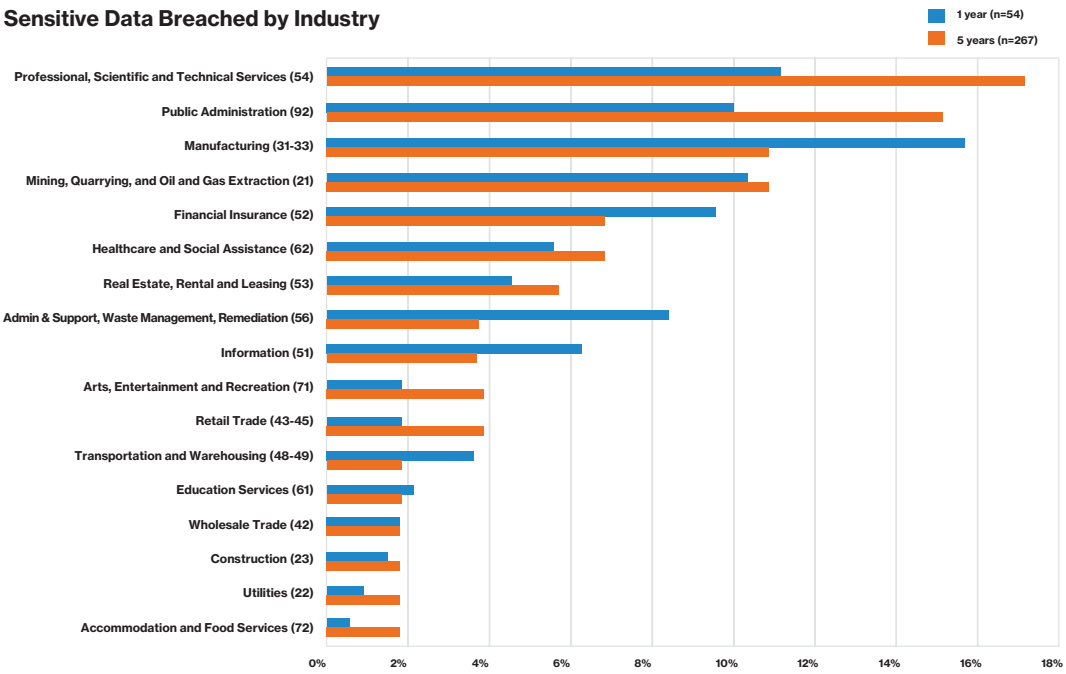


Figure 19.
Industries within Insider and Privilege Misuse Breaches Involving Select Data Varieties[1]

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 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.

[1] NAICS = North American Industrial Classification System (www.census.gov/eos/www/naics/) or (https://www.naics.com/naics-drilldown-table/)

Who are the Threat Actors?

Perhaps you'll recognize one or more of these insider threat actors. Most organizations have them:

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.

The Insider Threat Report shows business line managers and HR leaders how to develop early-warning systems to address potential insider threats before they result in catastrophic breaches.

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 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 imply an insider in conducting malicious activity. But taken as a whole they may be concerning, and attention should be paid.

Money, Fear and Fun: What Motivates Inside Actors to do Bad Things?

Cybercriminals targeting organizations from the outside are overwhelmingly motivated by financial gain: the rise of the Dark Web means it's easier than ever to monetize stolen data. And while financial gain can motivate insiders, our research shows they have a wider range of reasons for malicious acts. These can include boredom and curiosity, working around security controls to make a task more convenient or holding a grudge and seeking revenge:

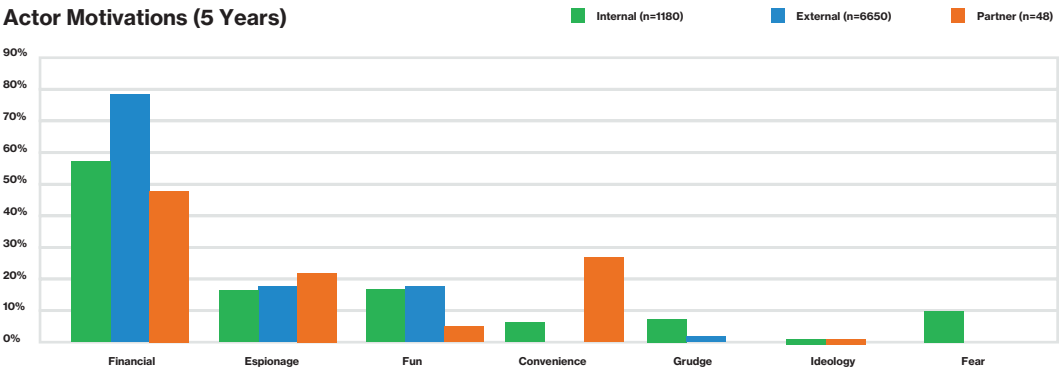


Figure 8.
Actor Motivations within Data Breaches

The Good News: You Aren't Powerless

From preparation to mitigation, detection to response, The Insider Threat Report provides extensive guidance on addressing risks from within. These include

Preparation and Mitigation

- Control and restrict access to trade secrets, customer data and other proprietary information on a need to know basis
- Increase monitoring and logging of sensitive areas, systems and data
- Monitor behavior including use of external storage devices and cameras and smartphones in sensitive areas
- Disable access for activities deemed inappropriate, malicious or otherwise posing organizational risk

Detection and Response

- Monitor suspicious network traffic such as unusual off-hours activity, volumes of outbound activity, and remote connections
- Keep baseline system images and trusted process lists; compare these standards 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 and rebuild affected systems

The Insider Threat Report offers many more countermeasures you and your teams can take to reduce potential risks – and avoid becoming yet another cybercrime headline.

The Cybersecurity Threat from Insiders is Real.

Protect your organization with actionable insights from the full Insider Threat Report.