proofpoint.

E-BOOK

The 10 Biggest and Boldest Insider Threat Incidents

2020-2021

proofpoint.com

Introduction

As the workplace quickly evolves, people are working from anywhere and accessing data everywhere. This shift has dramatically increased many organizations' exposure to cyber risk. Suddenly, CISOs must manage not just external threats, but countless risks from within.

In fact, 58% of CISOs believe that even though employees understand their role in protecting against cyber threats, they also pose the biggest risk.[2]

Insider threats are not always malicious. Many are due to negligence by well-meaning people who accidentally leak confidential or sensitive data. Others stem from compromised users who unknowingly fall victim to credential compromise or malware that infects and takes control of their devices.

Most organizations spend significant time and resources understanding and mitigating external threats. Unfortunately, few make the same investment in learning about internal threats. As a result, organizations don't know what insider threats look like—let alone how to combat them.

This e-book reviews 10 headline-grabbing insider threat incidents that provide a useful glimpse into the reality of this growing threat. We explore five key elements within each incident:

- What happened
- Who is behind the insider incident—and why
- Why insider incidents may be intentional, accidental or the result of account compromise
- How much these incidents cost the organization they hit
- Lessons learned from each of these examples to ensure you can better protect your organization

More than

90%

of successful cyberattacks require some level of human interaction.[1]

[1] Proofpoint. "2021 Voice of the CISO Report." June 2021.

[2] ibid.

01 ConocoPhillips

A New Meaning of Friendship

A ConocoPhillips employee created fraudulent invoices to trick the oil giant into paying a friend's business more than $3 million. The actions were part of a larger embezzlement scheme that totaled nearly $7.3 million.

Victim: ConocoPhillips

Vertical: Energy

Insider Risk Categories: Intentional/Malicious, Employee, Fraud

$7.3M

in total damages in embezzlement scheme

Lessons Learned

A robust insider threat management (ITM) platform can help detect and prevent supply chain risks by recognizing fraudulent invoices and requests before it's too late.

Identifying high-risk insiders, and ensuring your organization is properly monitoring their activity, can help reduce the mean time to detect and resolve an insider threat incident.

Though malicious insider threats are carried out by someone on the inside, they rarely work alone. In most cases, nefarious actors outside the organization are also involved.

Learn More

ALASKA PUBLIC MEDIA | US DEPARTMENT OF JUSTICE

02 Postbank

Don't Mind Me ... Just Copying Some Keys

South Africa's Postbank fell victim to a major insider-caused security breach when multiple employees copied the primary encryption key.

Victim: Postbank

Vertical: Financial Services

Insider Risk Categories: Intentional/Malicious, Employee, Encryption Keys

$58M

Cost to Replace Bank Cards

$3.35M

Cost of Damages

Lessons Learned

Robust ITM involves detection, response and user training to meet financial compliance requirements.

Time is of the essence when it comes to alerting, investigating and resolving insider incidents.

Insider threats don't always act alone; sometimes, a group can band together to execute fraud on a massive scale. That's what happened here.

Learn More

CPO MAGAZINE | ZDNET

03 US Military

Studying Gone Very Wrong

US soldiers trying to memorize the security protocols around nuclear weapons protections unknowingly leaked a significant amount of sensitive information by using an unsecured flashcard learning app.

Victim: US Military

Vertical: Defense

Insider Risk Categories: Negligent Employee, Compromised Defense Systems

US soldiers unknowingly exposed nuclear weapons secrets publicly for

8 years

Lessons Learned

Even the most well-intentioned employee can inadvertently leak sensitive information, putting the business—or this case, national security—at risk.

Every user should be educated about cybersecurity best practices. Those who act in especially risky ways or have higher levels of access to sensitive data may require targeted training and additional monitoring.

The longer an insider threat goes undetected, the higher the risk of leaked data getting into the wrong hands, the more time and effort required to contain the leak and the greater damage that can result.

Learn More

BELLINGCAT | THE VERGE

04 Microsoft

Microsoft Misconfiguration Leads to Big Mistake

Microsoft stored customer information in unsecured servers, leading to the exposure of 250 million customer records over the course of 14 years.

Victim: Microsoft

Vertical: Technology

Insider Risk Categories: Intentional/Malicious, Employee, PII Information Leaked, Loss of Customer Trust

14 years

Length of time customer data was exposed

Lessons Learned

To err is human. But when tech behemoths like Microsoft mess up, those affected may not be so understanding. A misconfiguration of this magnitude calls into question the security and privacy practices of large organizations, even raising flags around various compliance initiatives worldwide.

Mitigating the potential for data loss requires a solution that recognizes misconfigurations early and a rapid-remediation plan to act on that insight.

Whether intentional or negligent, data loss can create big problems for any organization, ranging from financial losses, cost to reputation and brand damage.

Learn More

FORBES | ENGADGET

05 Twitter

Twitter Duped by a 17-Year-Old Floridian

A cyber criminal ring led by a Florida teenager coerced a Twitter employee to give up credentials for corporate administrative tools, leading to takeovers of verified accounts used in a Bitcoin-promotion scam.

Victim: Twitter

Vertical: Technology

Insider Risk Categories: Employee, Credential Theft, Social Engineering, Scam, Fraud

$117K

Stolen from Customers

Lessons Learned

The attack triggered scrutiny about Twitter's security and privacy practices, straining users' trust and tarnishing the social media giant's reputation.

Work-from-home policies may be part of the reason it was so easy for the scammers to infiltrate and convince an insider to give up credentials—a warning for remote teams.

Least-privilege access and careful monitoring of high-risk, high-privilege users are key to avoiding a similar attack at your organization.

Learn More

NYTIMES | CNN | THE VERGE

06 Ellsworth County Rural Water District

Don't Drink the Water

A former employee at the Ellsworth County Rural Water District No. 1 in Kansas remotely accessed the water district's computer system and tampered with the disinfecting and cleaning process. By doing so, he risked the safety of the drinking water for the 1,500 retail customers and 10 wholesale customers across eight Kansas counties.

Victim: Ellsworth County Rural Water District

Vertical: Utilities

Insider Risk Categories: Intentional/Malicious, Employee, Network and Systems Disruption

25 years

Maximum number of years in prison the former employee faces

Lessons Learned

Organizations must implement an effective offboarding process to ensure that former employees cannot access an organization's network. This includes blocking remote access as well as increasing password security.

Monitoring remote access to any network is an essential part of a robust cybersecurity plan, ensuring that only those with authorized access can log in. Any unauthorized user should be flagged and prevented from accessing any information.

Deploying an ITM program can help. By monitoring data movement, you can quickly and more accurately spot malicious activity and take steps to stop or mitigate the damage.

Learn More

US DEPARTMENT OF JUSTICE | ARS TECHNICA

07 Le Figaro

A Newspaper Makes Headlines—and Not in a Good Way

French newspaper Le Figaro's accidental data leak—caused by a third-party hosting firm's poor security hygiene—exposed 7.4 billion records.

Victim: Le Figaro

Vertical: Media and Communications

Insider Risk Categories: Third Party, Accidental/Negligent, Data Loss

$7.4B

User Records Exposed

Lessons Learned

Outside vendors must meet strict risk assessments before they are used to store or traffic valuable information about users.

Attacks often morph from data theft to more complex and dangerous attacks that target internal systems, so having early warning systems in place is key.

Database leaks are one of the most common insider threat types. Make sure yours are properly configured and that monitoring is in place to detect leaks.

Learn More

INFOSECURITY MAGAZINE | BLEEPING COMPUTER

08 Morrisons

Cleanup in the Data Security Aisle

A senior internal auditor at U.K. grocery chain Morrisons leaked the payroll data of almost 100,000 employees. He was convicted of fraud in a case that made its way up to the U.K. Supreme Court.

Victim: Morrisons

Vertical: Retail

Insider Risk Categories: Intentional/Malicious, Employee, Data Exfiltration, Revenge, Fraud

£100K

Employees' Payroll Data Leaked

£2M

Cost to Business

Lessons Learned

While Morrisons escaped liability for its employee's actions in this case, insider threats can expose businesses to significant liability.

Deploying an insider threat detection platform reduces the odds of an employee successfully exfiltrating and exposing sensitive information.

Internal auditors are supposed to be an organization's "watchdogs." Just be sure someone is watching the watchdogs, who have highly privileged access that can be abused.

The Supreme Court ruled that Morrisons would not be held liable for the malicious employee's behavior. But the ruling also made clear that a business can be held accountable for employees' actions when their job responsibilities and the nefarious activity are closely connected. The incident shows that recognizing high-risk employees early and effectively monitoring their data use are critical.

Learn More

THE GUARDIAN | NATIONAL LAW REVIEW | INFORMATION AGE | PEOPLE MANAGEMENT

09 Vertafore

Can I See Some ID?

Negligent employees at insurance software maker Vertafore exposed a Texas Department of Motor Vehicles database after storing files in an unsecured external storage service. The incident led to a class-action lawsuit.

Victim: Vertafore

Vertical: Insurance

Insider Risk Categories: Third Party, Negligent Employee, Customer Data Leaks

27.7M

Number of Texas Drivers whose data was exposed

Lessons Learned

Training employees on proper cybersecurity processes and protocols is critical for any organization. In this case, a lack of training on how to properly store sensitive information resulted in the class-action lawsuit after the data was exposed.

Even well-intentioned employees can make mistakes. That's why it's critical to have a robust ITM program in place to ensure data loss can be prevented by monitoring who gains access to sensitive information and how that data moves.

Ensure all your third-party partners and vendors are adhering to the cybersecurity guidelines you've established as your baseline of operation.

Learn More

INFOSECURITY | ZDNET | TOP CLASS ACTIONS

10 Stradis

PPE Shipments Sabotaged During the Covid-19 Crisis

The fired ex-VP of finance at Georgia-based Stradis Healthcare deleted or altered more than 115,000 data records, disrupting shipments of personal protective equipment (PPE) during the early days of U.S. pandemic response.

Victim: Stradis

Vertical: Healthcare

Insider Risk Categories: Intentional/Malicious, Employee, Privilege Abuse, COVID-19, Revenge

$5K

Cost to Business

Lessons Learned

Creation of fake accounts is a key insider threat indicator that should be quickly flagged by security software and reviewed internally.

Employees with a disciplinary history—especially those involving access and system abuse— should be flagged as high-risk and monitored with extra caution. Revenge is a common motive for malicious insiders.

Employees with a high level of privilege, such as a VP of finance, should also automatically receive more scrutiny to ensure they do not abuse their privileges.

Learn More

BANKINFOSECURITY | NEWSBREAK

Conclusion and Recommendations

As these examples illustrate, insider threats can come in all shapes and sizes. That's why it's critical to understand the "who," "what," "how," "why" and "when" of an insider incident.

Who

Understanding the "who" helps organizations know how to move forward. With a modern, people-centric approach, organizations can gain deeper and more accurate insights into:

- Who has access to specific data
- What they're doing with it
- How they're sharing it

This context empowers organizations to explore the right next step when responding to an insider incident, whether it's internal training, discipline or bringing in law enforcement.

What and How

Knowing exactly what occurred before, during and after an incident is crucial to response and recovery. Only a purpose-built ITM solution that takes a modern approach to DLP can give you full visibility and context into the play-by-play of "what" happened and "how".

By monitoring any data movement or risky behaviors across files, apps, and endpoints, organizations gain insight into the sequence of events so all relevant internal departments can quickly understand the context of the incident. Having this irrefutable evidence can help exonerate well-meaning insiders or prosecute malicious actors—with no lingering questions about "what" really happened.

Why

Insider threat motivations can range from greed and financial gain to revenge, as is the case in several of these examples. But sometimes these incidents are simply the result of negligence. Understanding the "why" is key to the right response.

When

One of the key factors in the cost of an insider threat incident is how long it lingers. As some of these examples show, incidents sometimes go unnoticed for days, weeks or even years. The more time an insider has within a system, the more damage that person can do. The earlier organizations can identify and respond to an incident, the less damage they suffer to their reputation and bottom line.

Next Steps

Every insider threat is unique. That's why detecting, investigating and responding to each one requires a distinct approach. The key is to invest in a purpose-built insider threat management platform built on a cloud-based modern architecture to protect against data loss, financial costs, and brand damage from insiders acting maliciously, negligently or unknowingly. An ITM platform helps reduce data loss from insider risks and external threats, streamline your team's workflow and speed up incident detection and response.

Organizations are embracing the cloud, a work-from-anywhere culture and innovation as core values. It's time your ITM solution does, too, so you can protect your business from the inside out.

Learn More

To find out how Proofpoint can help your organization manage insider risk, visit **proofpoint.com/us/products/information-protection/insider-threat-management**.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0512-003-01-02 08/21