proofpoint.

The 10 Biggest & Boldest

Insider Threats of 2019 and 2020

01

Easy employee access to sensitive databases and

large-scale credential theft

Canadian Desjardins Group hit with a massive insider-caused data breach after an IT employee stole bank customer information using multiple employees' credentials.

Company: Desjardins Group | **Industry:** Financial Services | **Insider Risk Categories:** Database Access Control Issues, Credential Sharing, Malicious Employee

Lessons Learned:

Protect valuable personally identifiable information (PII) such as bank account details using an ITM platform.

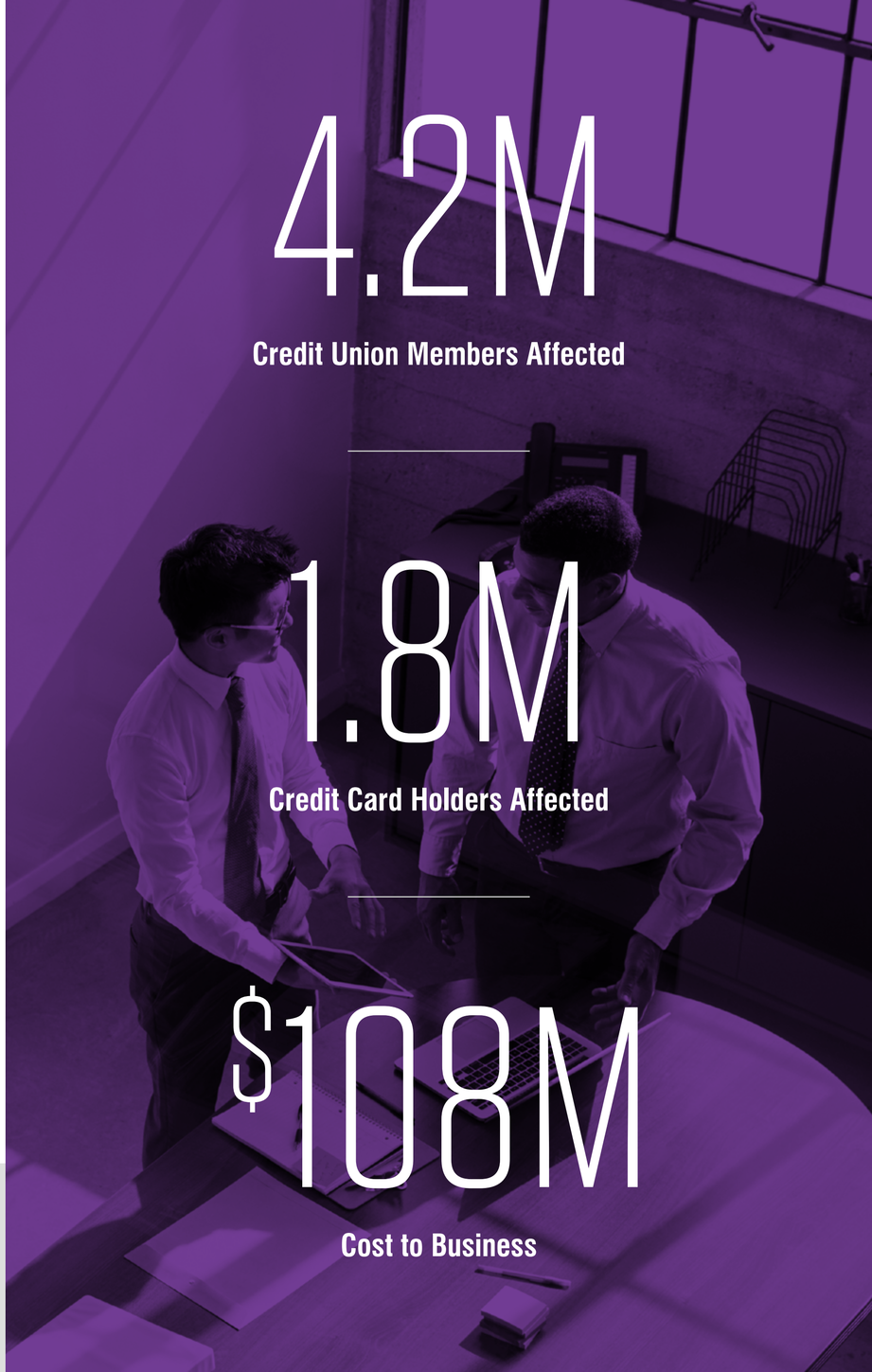
Preventative access controls aren't enough to stop credential sharing.

Detection of shared credential usage and risky database activity should be part of your ITM platform.

Compliance is a basic requirement. Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada applies to data security.

Learn More:

CBC | PANDA SECURITY | INFOSECURITY MAGAZINE | REUTERS



4.2M

Credit Union Members Affected

1.8M

Credit Card Holders Affected

$108M

Cost to Business

02

Don’t mind me...

just copying some keys

South African Postbank fell victim to a major insider-caused security breach when multiple employees copied the master encryption key.

Company: Postbank | **Industry:** Financial Services | **Insider Risk Categories:** Intentional/Malicious, Employee, Encryption Keys

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 | SECURITY BOULEVARD

03

The case of the

missing trade secrets

Cybereason claimed in 2020 that its former director of product management stole sensitive intellectual property on his way to a new role at competitor SentinelOne.

Company: Cybereason | **Industry:** Technology | **Insider Risk Categories:** Intentional/Malicious, Employee, IP Theft, Privilege Abuse

Lessons Learned:

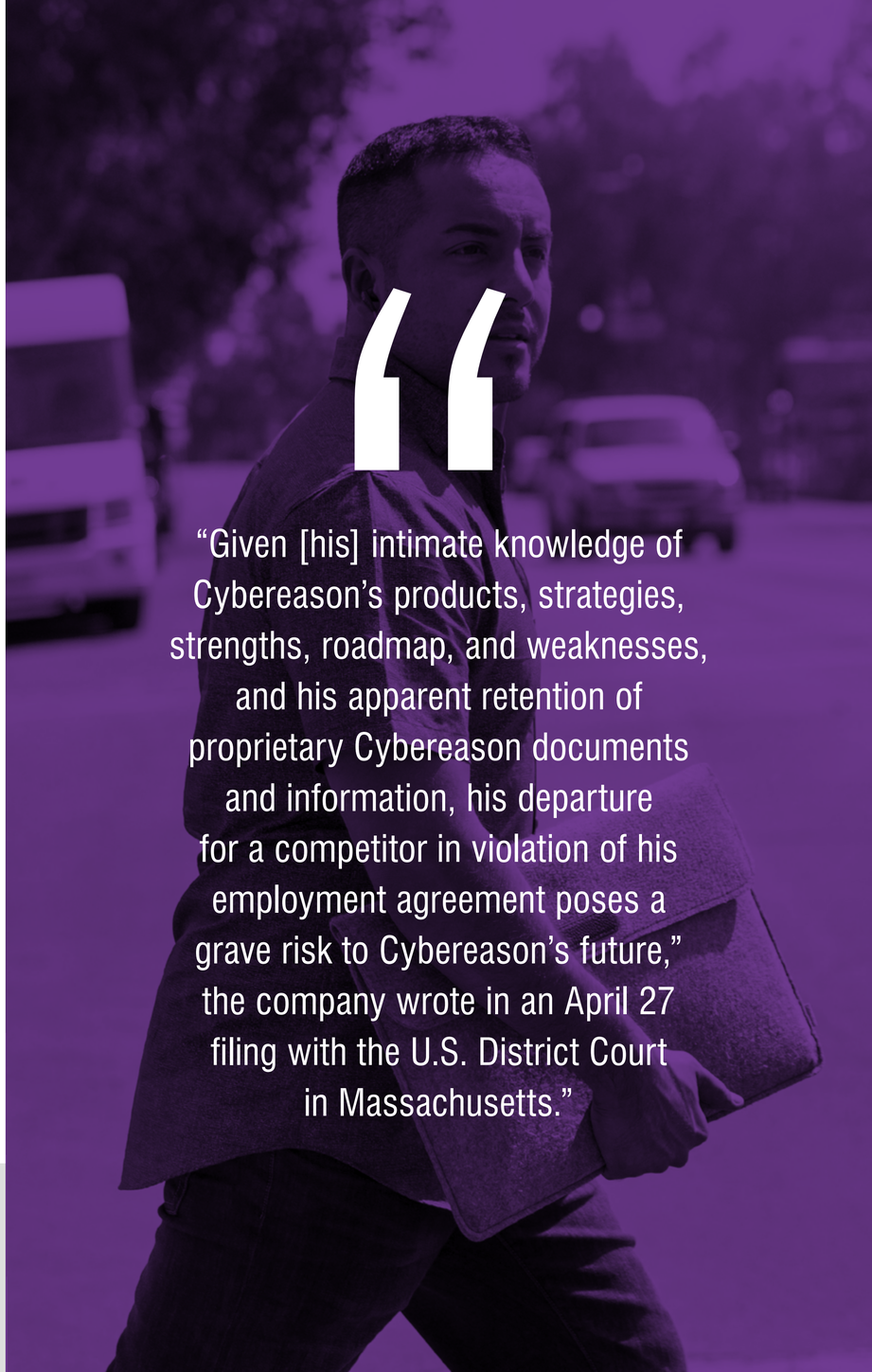
Senior product managers help build intellectual property and trade secrets, and they are high-risk insiders.

Alerting on early insider threat indicators—such as copying files to personal cloud storage or using USB drives to exfiltrate data—is key to stopping insider threats.

A robust ITM platform can not only detect what happened before, during, and after an insider incident, but also prevent insiders from covering their tracks.

Learn More:

CRN | SECURITY DISCOUNTS



“Given [his] intimate knowledge of Cybereason’s products, strategies, strengths, roadmap, and weaknesses, and his apparent retention of proprietary Cybereason documents and information, his departure for a competitor in violation of his employment agreement poses a grave risk to Cybereason’s future,” the company wrote in an April 27 filing with the U.S. District Court in Massachusetts.”

04

What happens when security companies

aren’t so secure?

A Trend Micro employee sold data belonging to 68,000 customers to a malicious third party who used the data for scam phone calls.

Company: Trend Micro | **Industry:** Technology | **Insider Risk Categories:** Intentional/Malicious, Employee, Data Exfiltration, Scam, Third Party

Lessons Learned:

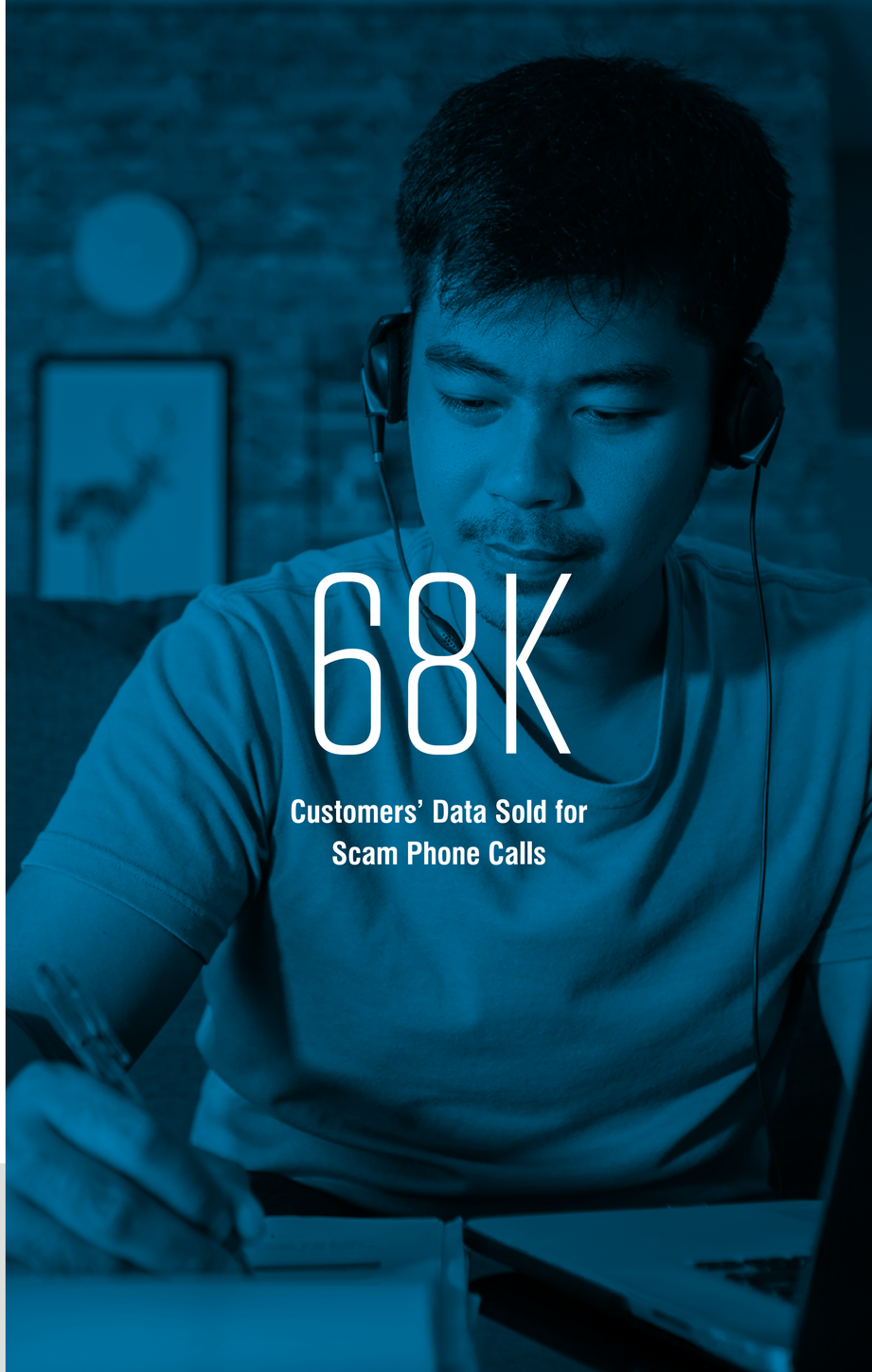
Even security companies are vulnerable to insider threats. In fact, no industry or company is immune to this insidious threat type.

Sensitive data lives in many places in any given organization, so blocking is not effective. Alerting and contextual threat intelligence are key.

Proactivity is of utmost importance. The last thing an organization wants is to learn about a breach from its customers.

Learn More:

THREATPOST | ZDNET | OBSERVEIT



05

Twitter hacked by

a 17-year-old Floridian

A group of hackers led by a teenager coerced a Twitter employee to give up credentials for administrative tools, leading to verified account compromises and a Bitcoin scam.

Company: Twitter | **Industry:** Technology | **Insider Risk Categories:** Employee, Credential Theft, Social Engineering, Scam, Fraud

Lessons Learned:

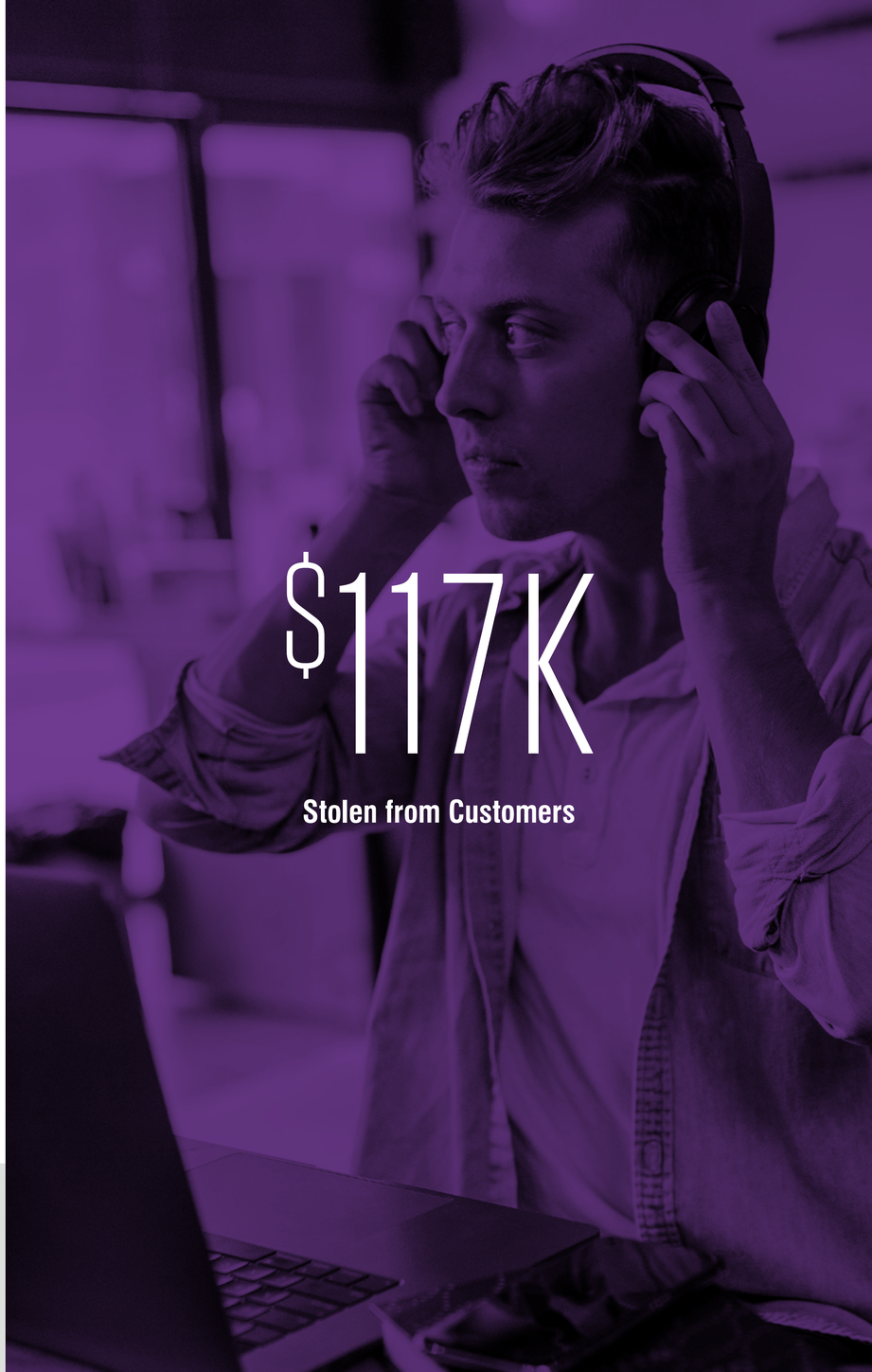
Attacks like these can call reputations into question and spark debate and scrutiny about the security and privacy practices of Twitter and other major services.

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

PPE shipments sabotaged

during the COVID-19 crisis

The former VP of finance at Georgia-based Stradis Healthcare sabotaged shipments of personal protective equipment (PPE) during the early days of U.S. pandemic response in an apparent act of sabotage.

Company: Stradis | **Industry:** Healthcare | **Insider Risk Categories:** Employee, Privilege Abuse, Intentional/Malicious, COVID-19, Revenge

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

07

Are you sure you trust

that contract IT team?

An IT agency hired by Singapore's SingHealth caused a data breach involving records for 1.5 million patients by failing to follow security best practices and ignoring warning signs.

Company: SingHealth | **Industry:** Healthcare | **Insider Risk Categories:** Accidental/Negligent, Third Party, Data Exfiltration, Poor Security Hygiene

Lessons Learned:

SingHealth's contractor neglected Singapore's stringent regulatory requirements for privacy and security via the Personal Data Protection Act.

Insider threats can also originate with third parties, including IT vendors. Insider threat monitoring must cover all insiders.

A robust combination of insider threat technology, security awareness training and responsible systems management is required for a complete security strategy.

Learn More:

HEALTHITSECURITY | STRAITS TIMES

08

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.

Company: Le Figaro | **Industry:** Media and Communications | **Insider Risk Categories:** Third Party, Accidental/Negligent, Data Loss

Lessons Learned:

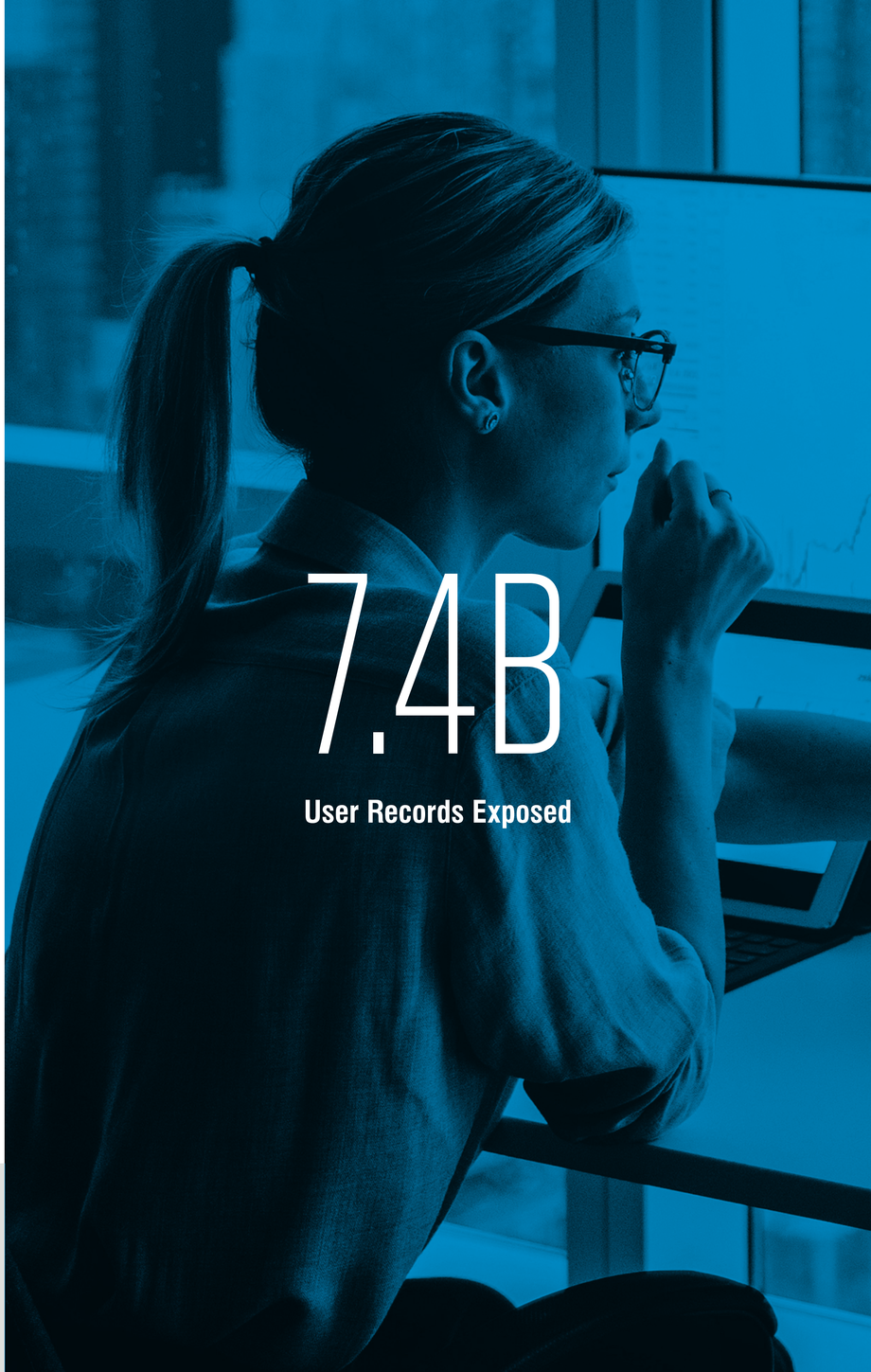
Third-party vendors must meet strict risk assessments before they are used to store or traffic valuable information about users.

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

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

Learn More:

INFOSECURITY MAGAZINE | BLEEPING COMPUTER



09

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 and found himself convicted of fraud in a case that made its way up to the U.S. Supreme Court.

Company: Morrisons | **Industry:** Retail | **Insider Risk Categories:** Employee, Data Exfiltration, Intentional/Malicious, Revenge, Fraud

Lessons Learned:

While Morrisons escaped liability for its employee's actions, that is not always how things play out in the courts. Insider threats open up businesses to significant liability.

Implementing an insider threat detection platform decreases the odds that an employee can successfully exfiltrate and expose sensitive information.

Internal auditors may be thought of as "watchdogs," but it's key to also watch the watchdogs—who in reality have massive access and potential for abuse.

Learn More:

THE GUARDIAN | NATIONAL LAW REVIEW | INFORMATION AGE

10

Chaos in the warehouse

After quitting, a former IT admin at an Atlanta-based building products distributor committed sabotage by changing router passwords and shutting down the central command server.

Company: Building Products Distributor | **Industry:** Manufacturing & Logistics | **Insider Risk Categories:** Employee, Privileged User, Revenge, Multi-Stage Sabotage, Intentional/Malicious

Lessons Learned:

Many security tools miss the signs of insider threat activity, a strong argument for investing in a purpose-built ITM solution.

IT managers have significant privileges and should be considered high-risk users. ITM tools should be used to monitor their activities both during and after employment.

More security precautions should be implemented around systems and devices that have the power to bring a company down—such as central command servers.

Learn More:

BANKINFOSECURITY

LEARN MORE

proofpoint.com

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity 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**.

LEGAL DISCLAIMER

This document does not represent legal interpretaion on corporate regulation and policy. Whilst efforts have been made to ensure maximum accuracy, this document does not substitute for the regulation. Only the regulation and its official interpretation can provide complete and definitive information regarding requirements. This document does not bind ObserveIT, a division of Proofpoint, and does not create any rights, benefits or defenses, substantive or procedural, that are enforceable by any party in any manner.

proofpoint.

08/20