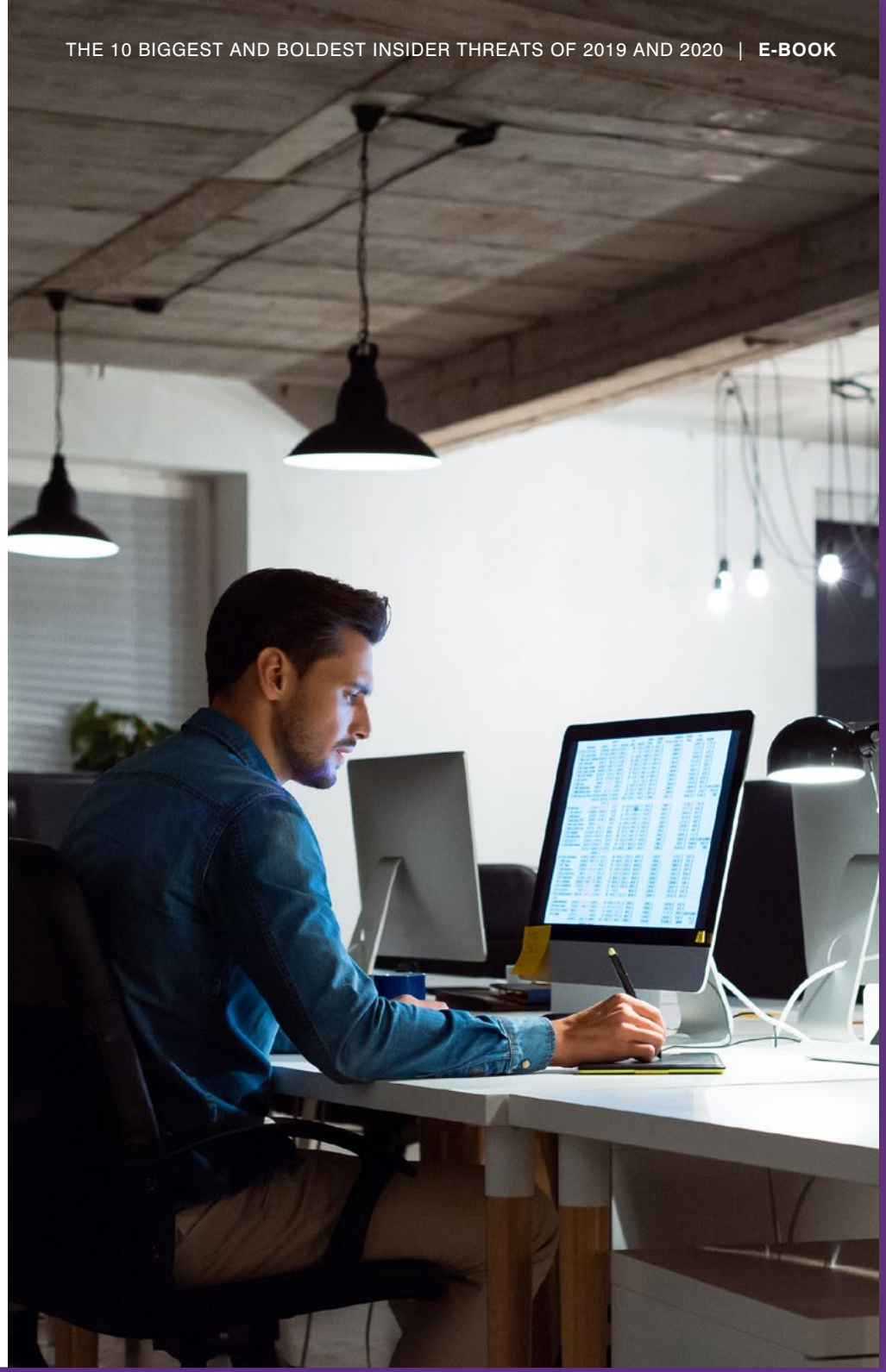
proofpoint.

The 10 Biggest and Boldest

Insider Threats of 2019 and 2020



INTRODUCTION

Over the last two years alone, insider security incidents have jumped 47%, with the average cost per incident up 31%. [1]

That risk is only increasing in an era of remote working and distributed teams. Without a holistic security strategy in place, organizations face insider-caused breaches from negligent, malicious and compromised insiders.

And they aren't just employees. Anyone with insider access—including outside contractors, consultants and vendors—can pose an insider risk. Despite the risk, most organizations do not have a formal insider threat management (ITM) program in place.

This e-book reviews 10 headline-grabbing insider threat incidents that provide a useful glimpse into the reality of this growing threat. (Some of these occurred or began before 2019, but all have been disclosed or prosecuted in 2019 or 2020.) We explore:

- What these incidents look like
- Who is behind them—and why
- Why insider incidents may be intentional, accidental or the result of account compromise
- How much they cost the organizations they hit
- What we can learn from them to better protect your organizations

Insider threats can happen anywhere, anytime. Studying real-world examples is key to understanding how they play out so you can shore up your own defenses.

[1] Ponemon. "Cost of Insider Threats Global Report." February 2020.

01

Customer Data Theft Perpetrated by Insiders

Two Shopify support employees stole data from more than 100 merchants that use the platform. The breach resulted in potential exposure of consumers' personal information.

Victim: Shopify

Vertical: Financial Services, E-commerce

Insider Risk Categories: Database Access Control Issues, Malicious Employee, Data Loss

Lessons Learned

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

Preventative access controls aren't enough to stop insiders from stealing data.

Detection of risky database activity should be part of your ITM platform.

Support staff should be considered potential insider threats and monitored using an ITM solution.

Learn More

BLOOMBERG | HACKREAD

02

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 master encryption key.

Victim: Postbank

Vertical: Financial Services

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

Lessons Learned

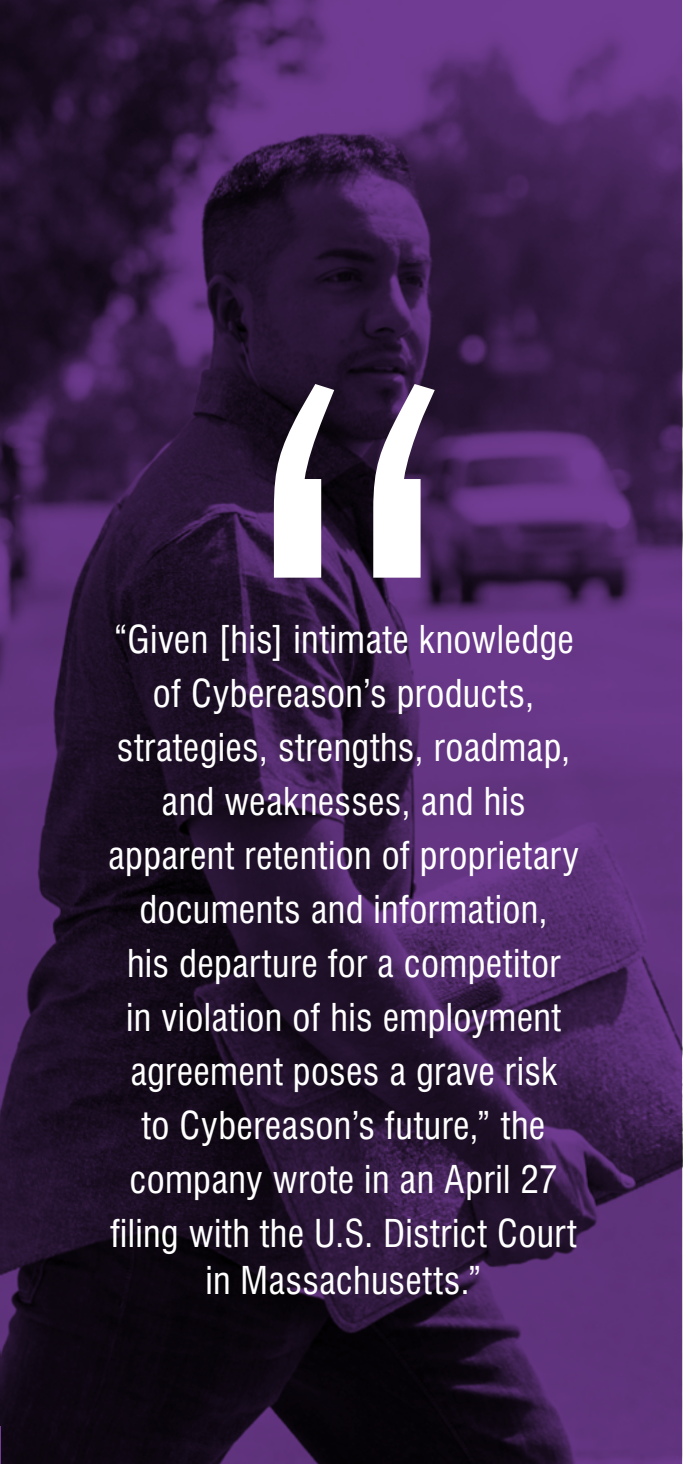
Robust ITM involves detection, response and user training to meet financial compliance requirements.

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



"Given [his] intimate knowledge of Cybereason's products, strategies, strengths, roadmap, and weaknesses, and his apparent retention of proprietary 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."

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.

Victim: Cybereason

Vertical: Technology

Insider Risk Categories: Intentional/Malicious, Employee, IP Theft, Privilege Abuse

Lessons Learned

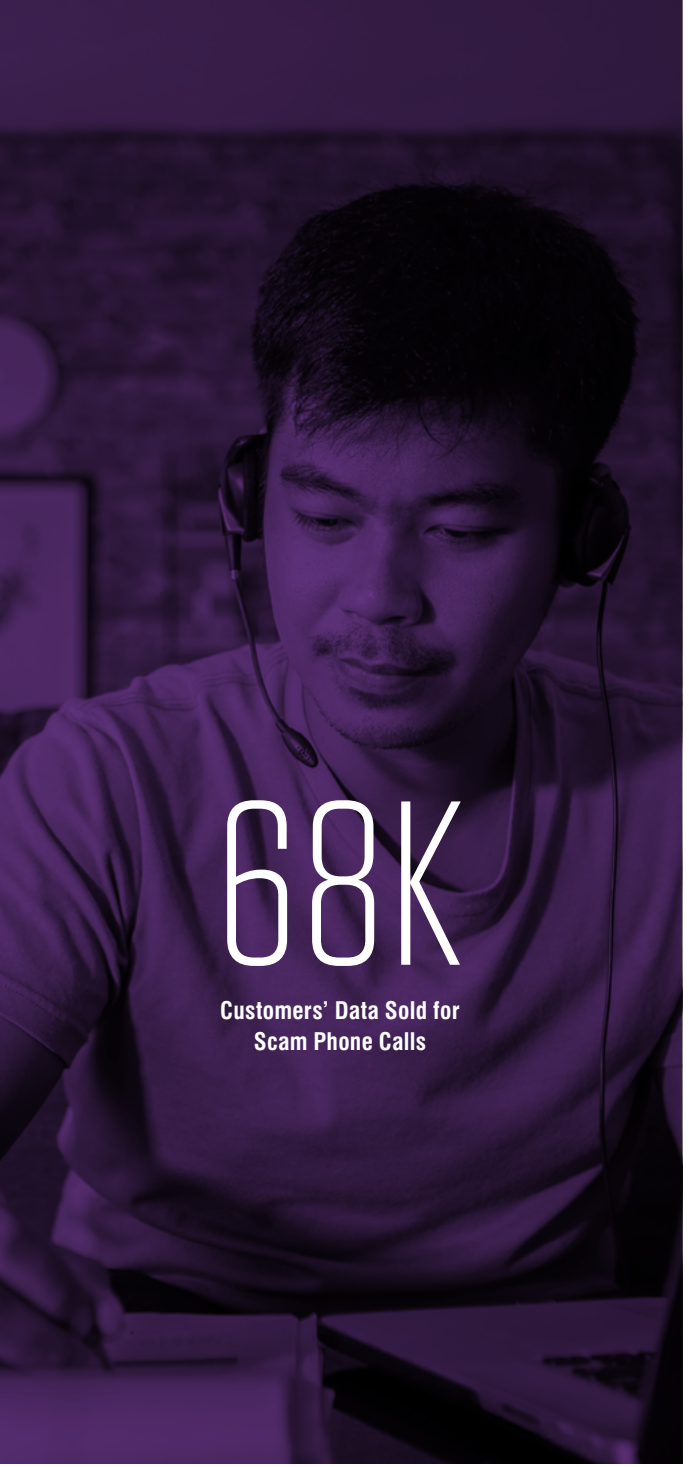
Senior product managers help build intellectual property and trade secrets, and they are high-risk insiders.

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



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.

Victim: Trend Micro

Vertical: Technology

Insider Risk Categories: Intentional/Malicious, Employee, Data Exfiltration, Scam, Third Party

Lessons Learned

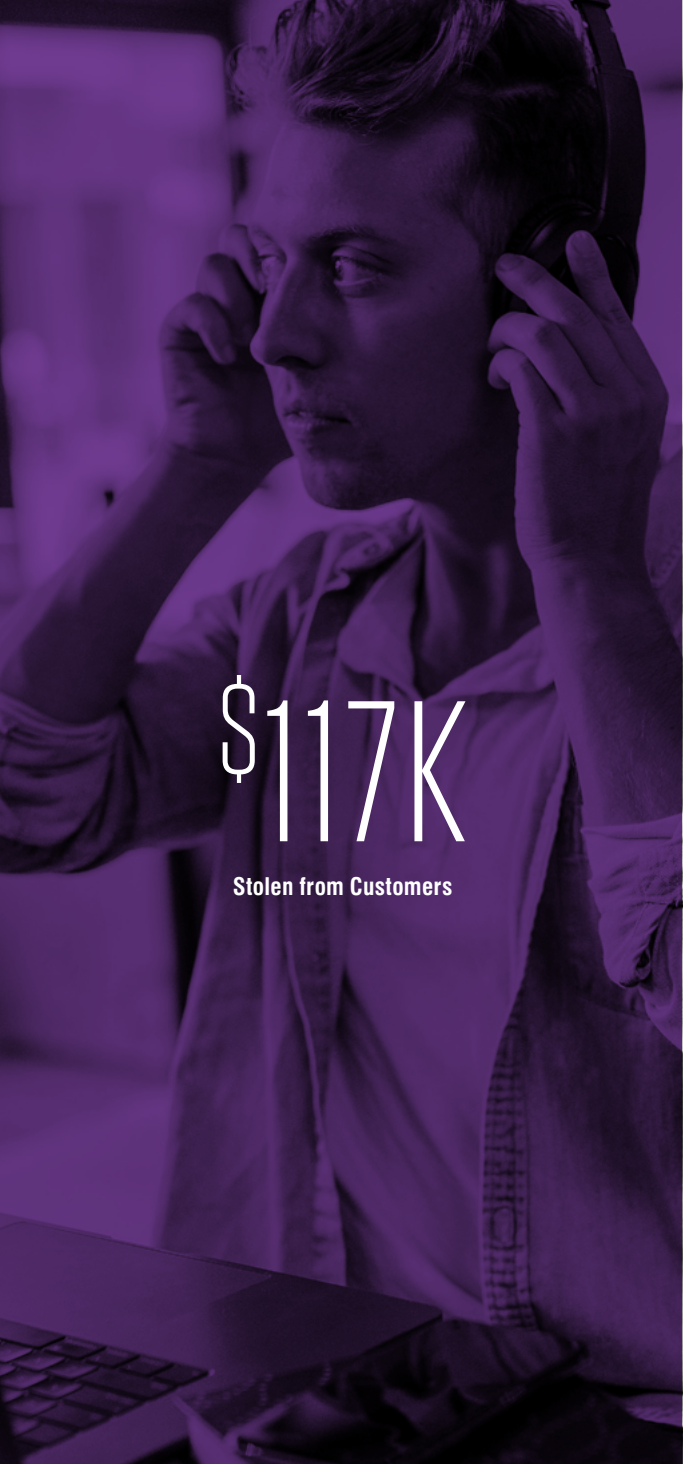
Even security companies are vulnerable to insider threats. In fact, no industry or company is immune to this insidious threat type.

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.

Victim: Twitter

Vertical: 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 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

Lessons Learned

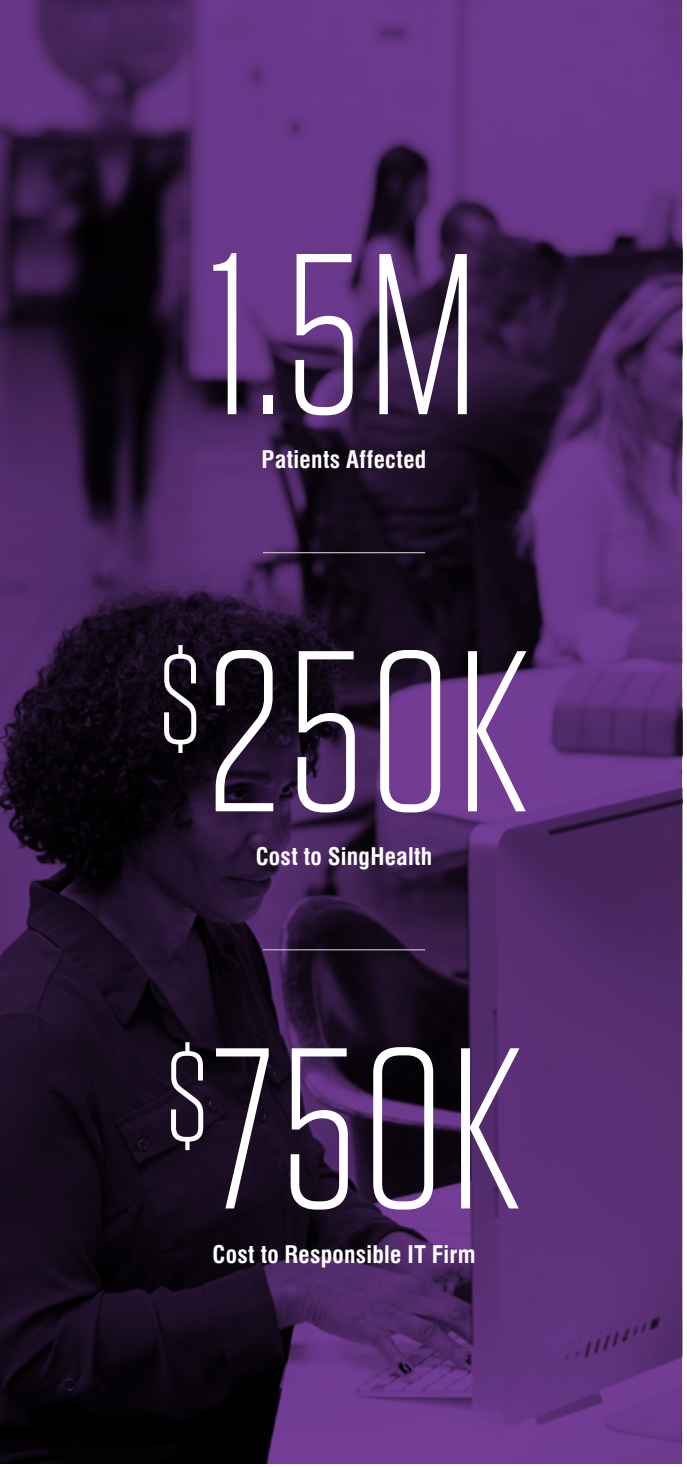
Creation of fake accounts is a key insider threat indicator that should be quickly flagged by security software and reviewed internally.

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.

Victim: SingHealth

Vertical: Healthcare

Insider Risk Categories: Accidental/Negligent, Third Party, Data Exfiltration, Poor Security Hygiene

Lessons Learned

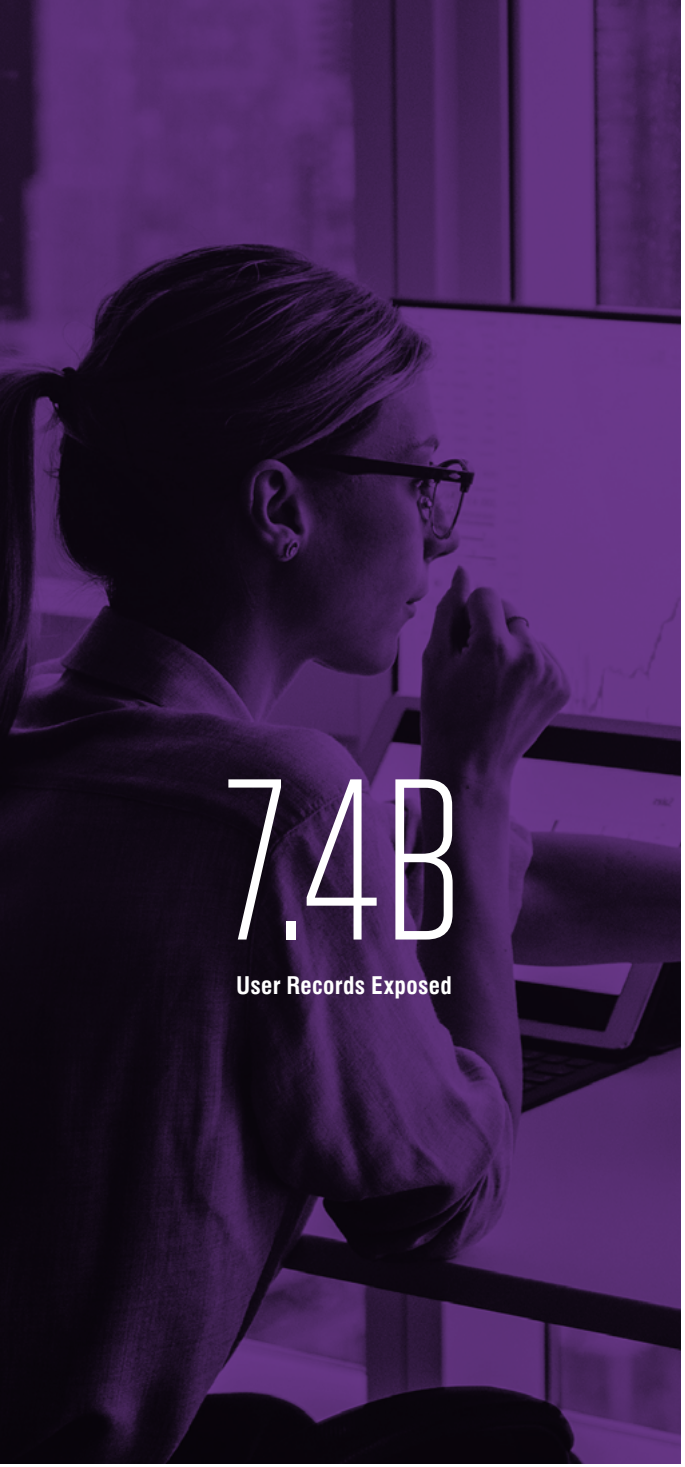
SingHealth's contractor neglected Singapore's stringent regulatory requirements for privacy and security via the Personal Data Protection Act.

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.

Victim: Le Figaro

Vertical: 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.

Victim: Morrisons

Vertical: Retail

Insider Risk Categories: Intentional/Malicious, Employee, Data Exfiltration, 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.

Victim: Building Products Distributor

Vertical: Manufacturing & Logistics

Insider Risk Categories: Intentional/Malicious, Employee, Privileged User, Revenge, Multi-Stage Sabotage

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

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", "why" and "when" of an insider incident.

Who

Understanding the "who" helps organizations know how to move forward. That may include internal training, discipline or bringing in local or national law enforcement.

What and How

Knowing exactly what went down before, during and after an incident is crucial to response and recovery. Only a purpose-built ITM solution can give you full visibility and context into the play-by-play of what happened and how. Having this irrefutable evidence can help exonerate well-meaning insiders or prosecute malicious actors—with no lingering questions about "what" really happened.

Why

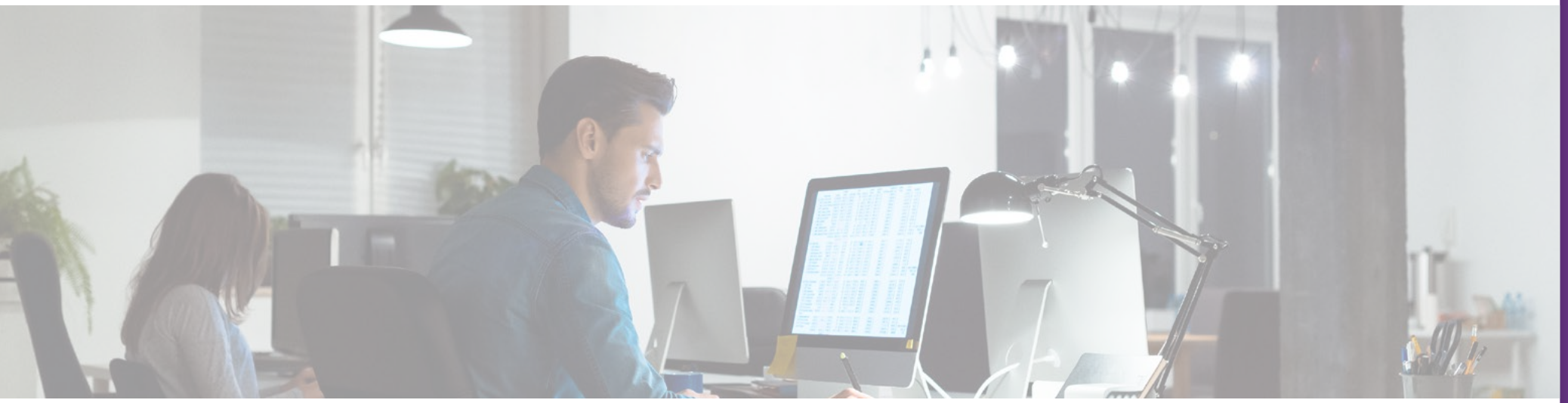
Insider threats can be motivated by greed and financial gain, as is the case in several of these examples. Other times malicious insider threats are motivated by revenge or a desire to take valuable IP with them to a new role. But sometimes these incidents are simply the result of negligence. Understanding 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 months. 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 that protects against data loss, malicious acts, and brand damage from insiders acting maliciously, negligently or unknowingly. So you can protect your business from risk from the inside out.



LEARN MORE

For more information, visit **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**.

proofpoint.

0512-003-01-01 10/20