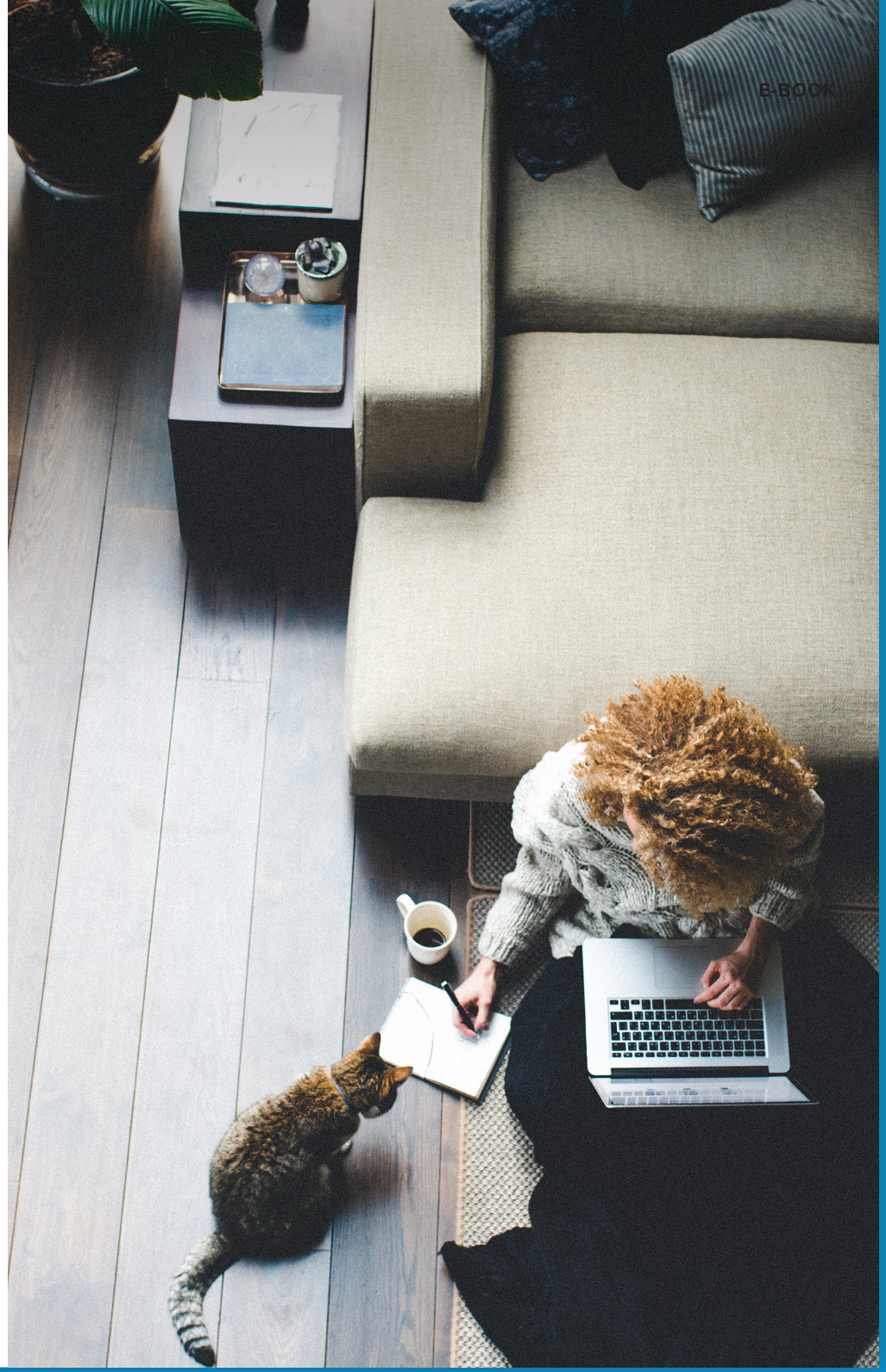
proofpoint.

The Data Breach is Coming from Inside the House

Real-Life Tales of Data Loss, Insider Threats and User Compromise



Introduction

Data doesn't lose itself. People lose it. It may start with an accidental file share. It may be a case of malicious insider sabotage. It can be the result of a misconfigured server or compromised user. In any of these scenarios, data loss is a people problem.

Most IT departments have little visibility into people-caused data loss in today's distributed, cloud-first work environment—let alone have a handle on it. Today's major security and compliance challenges include:

- Cloud account takeovers
- Oversharing of data
- Unapproved cloud apps
- Insider threats

Any of them can lead to data loss, exposure or theft—and consequences.

This e-book examines five real-world data loss incidents. We'll explore what they have in common, dissect how they're unique and explain how they could have been prevented.

Industry
Travel/hospitality

Cause of incident
Cloud storage misconfiguration

Records exposed, lost, compromised or stolen
10 million

Business outcome
Brand damage, strained business partnerships, possible GDPR fines

Prestige Software (November 2020)

What happened

Prestige Software's travel booking platform, Cloud Hospitality helps power many of the travel booking sites you've probably used—Booking.com, Expedia, Hotels.com and Sabre, among others. Like many web-based services, Prestige runs on Amazon Web Services (AWS), the e-commerce giant's cloud platform.

Someone at the Spanish company misconfigured an AWS storage bucket. That mistake exposed 10 million log files, which included the full names, email addresses, national ID numbers and phone numbers of hotel guests.[1] The records included the credit card number, cardholder's name, CVV and expiration date of hundreds of thousands of customers.[2]

The company learned of the data exposure from an outside website consulting firm in November 2020; it fixed the problem within a day.

[1] *Infosecurity.* "Hotel Booking Firm Leaks Data on Millions of Guests." November 2020.

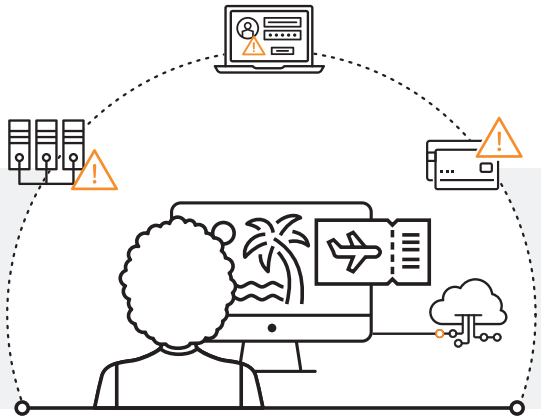
[2] Ibid.

Lessons learned

Cloud and infrastructure-as-a-service (IaaS) platforms are highly secure in many ways. But they present new kinds of risk that traditional DLP tools weren't built to manage. The typical organization may have tens or hundreds of IaaS accounts with workloads deployed on single or multiple cloud services. Due to data privacy regulations, they may have to store data on cloud repositories located in different regions of the world.

The lack of visibility into the gaps in your cloud security posture can make security and compliance difficult. Other threats such as account compromise and lack of well-trained staff can add to the complexity.

As Prestige's customers learned, the incident also shows why organizations shouldn't limit their DLP controls to employees. Outside contractors, vendors and partners often have insider-level access to critical data, making them potential data loss risks.



How to prevent it

A cloud access security broker (CASB) should be a critical part of your DLP arsenal. The right tool can spot configurations and settings that might pose a risk, control privileged access and protect data in the cloud.

Look for tools that help you:

- Identify misconfigurations in IaaS environments and recommend fixes
- Set policies to alert on unauthorized privileged user activities in SaaS and IaaS environments
- Set policies to block access from risky locations and networks and by known threat actors
- Apply risk-based controls to high-risk and high-privilege users including step-up authentication, managed-device policy rules and VPN enforcement
- Detect when a cloud account is compromised
- Investigate past activity and alerts, including any suspicious access to your federated IaaS services.

The lack of visibility into the gaps in your cloud security posture can make security and compliance difficult.

Industry
Healthcare

Cause of incident
Compromised user

Records exposed, lost, compromised or stolen
485,000[3]

Business outcome
Brand damage, strained business partnerships, potential HIPAA fines

EyeMed (July 2020)

What happened

EyeMed Vision Care is one of the largest providers of vison-related health insurance and services in the U.S. It serves more than 62 million members, managing employer-provided benefits plans through a network of thousands of eye doctors and eyewear retailers. EyeMed's mission: helping patients improve their vision and keep their eyes healthy.

In July 2020, the negative effects of a data breach came into full view when an EyeMed employee's email account was compromised. An outside attacker used the EyeMed account to send phishing emails to other people and, potentially, exposed personally identifiable information along with private health data.

The incident was reported to the U.S. Department of Health and Human Services' Office of Civil Rights in December.

The breach also affected EyeMed's business relationships with other healthcare providers, such as Aetna, Tufts and Blue Cross Blue Shield of Tennessee. These companies, which partner with EyeMed for their vision benefits, separately reported the breach to customers and authorities.

[3] Morgan Haefner *(Becker's Healthcare)*. "Email hack exposes data of 485K+ Aetna, Blue Cross members." December 2020.

Lessons learned

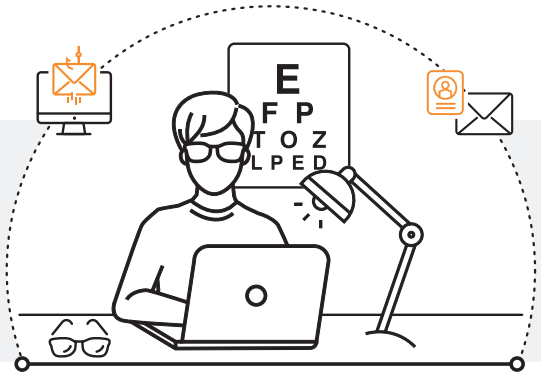
EyeMed said it blocked access to the compromised account soon after discovering the attack. It quickly deployed added security measures and beefed up its security awareness training efforts.

As the company learned, today's attacks target people, not just infrastructure. A compromised user account gives outside attackers insider-level access to all of the data, systems and resources within that user's sphere of privilege.

How to prevent it

Preventing an outsider-caused data breach requires a holistic, people-centric approach to data loss prevention. We recommend:

- Consolidating DLP, information protection, cloud and email security for more efficient and effective operations and a lower cost
- Training users to recognize and report credential phishing and other tactics attackers may use to gain access to their account
- Taking a people-centric view of users and the data they access with an approach that connects the dots between sensitive data, user behavior and outside threats
- Using prebuilt rules and templates, automation and advanced detection to speed up response, investigation and remediation efforts



Today's attacks target people, not just infrastructure.

Industry
Media

Cause of incident
OAuth misuse

Records exposed, lost, compromised or stolen
1.4 million[4]

Business outcome
Brand damage

Mashable (November 2020)

What happened

Mashable is one of the web's top tech and entertainment websites and a trusted source for news—including accounts of the latest data breaches.

In November 2020, the company found itself in the headlines when it disclosed that someone posted a copy of more than 5 gigabytes of internal data online.

The leak included a bevy of personally identifiable information: first and last names, home city or country, email addresses, gender, links to social media profiles, and month and day (though not the year) of their birthdate.

Threat researchers believe the perpetrator was a group called ShinyHunters, which has been linked to similar attacks against other websites.[5]

[4] Have I Been Pwned. "Pwned websites: Breached websites that have been loaded into Have I Been Pwned." Accessed April 2021.

[5] Waqas. "ShinyHunters hacker leaks 5.22GB worth of Mashable.com database." November 2020.

Lessons learned

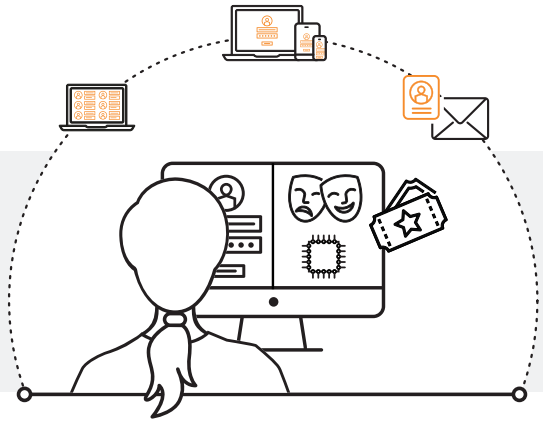
OAuth is an authorization protocol that enables a third-party application to obtain limited access to a cloud service. It enables a user's account information or data to be used by third-party apps without exposing the user's password.

Unfortunately, some OAuth permission requests are malicious. Cyber attackers can use OAuth access to compromise and hijack cloud accounts. And until the OAuth token is explicitly revoked, the attacker has persistent access to the user's account and data—even if the user changes the password or uses two-factor authentication (2FA).

How to prevent it

A cloud access security broker can help you discover third-party apps and scripts that have OAuth access to sensitive files and infrastructure. We recommend:

- Auditing new OAuth app requests, especially those coming from unknown sources
- Set up alerts for any third-party app or script requested by administrators, VIPs and other high-risk users, including users targeted more intensely in cyber attacks
- Blocking known malicious OAuth apps and requests
- Building out policies that automatically block certain categories of OAuth apps
- Set up alerts for any third-party app or script with rare or risky permissions such as "connect to external device"
- Inform users to choose and download apps from official app stores, not independent outside app stores.
- Notifying and educating users when they request blocklisted apps.



Cyber attackers can use OAuth access to compromise and hijack cloud accounts.

Industry
Technology

Cause of incident
Compromised user

Records exposed, lost, compromised or stolen
130 customer accounts compromised

Business outcome
Downtime for some users, brand damage, FTC fine of up to $250 million

TWITTER (JULY 2020)

What happened

Your cyber attack would have to be a pretty big deal if its targets included people like Joe Biden, Bill Gates, Barack Obama and Kanye and Kim Kardashian West.

The July 2020 breach of 130 Twitter accounts was a big deal. The now-U.S. president, software billionaire, former U.S. president and estranged celebrity couple were just a few of 130 high-profile Twitter users whose accounts were hijacked to promote a Bitcoin scam.

The attack began not with an attack of the celebrity accounts themselves but with the compromise of key Twitter employees.

According to company reports, attackers tricked high-privilege employees into providing account credentials. That, in turn, gave the attackers access to internal account support tools. From there, the attackers used celebrity accounts to trick fans into sending bitcoin—tweets promised victims twice the amount back as part of a promotion.

Investigators tracked down the alleged leader of the scheme, Graham Ivan Clark, who went by the name “Kirk” online. He was a 17-year-old recent high school graduate. Two other suspects, Mason John Sheppard, 19, of the United Kingdom, and Nima Fazeli, 22, of Orlando, Fla., were also arrested as accomplices.

Lessons learned

For Twitter, the attack "was a striking reminder of how important each person on our team is in protecting our service." Beyond direct financial costs and remediation, insider attacks can be especially damaging to your brand.

It was also a reminder that insider threats aren't always malicious or negligent employees. In fact, compromised users are the most damaging type of insider threat, costing victims 2.5 times as much per incident as those stemming from negligence.[6]

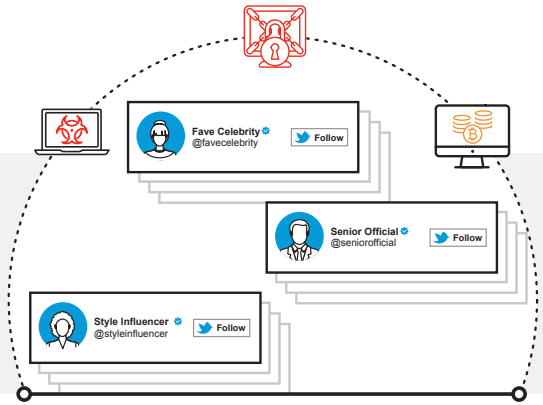
Work-from-home policies may be part of the reason it was so easy for the scammers to infiltrate and convince an insider to give up credentials—a warning for remote teams.

How to prevent it

Not every insider threat is a greedy insider looking for a payout or disgruntled worker seeking revenge. Many risks stem from negligent and compromised users who unwittingly pose as insider threats. Insider risk should be a major focus of every digital-driven businesses.

We recommend:

- Adopting least-privilege access policies to help contain the damage if an insider is compromised
- Monitoring high-risk, high-privilege users so that security and IT teams can quickly detect and respond when a user is compromised
- Conducting regular and targeted security awareness training that incorporates real-world threats and tactics
- Warning and educating users in real time when they make a mistake or before they attempt something malicious



Beyond direct financial costs and remediation, insider attacks can be especially damaging to your brand.

[6] *Ponemon.* "2020 Cost of Insider Threats: Global Report." April 2020.

Industry
Media

Cause of incident
Misconfigured cloud server

Records exposed, lost, compromised or stolen
7.4 billion

Business outcome
Brand damage

Le Figaro (April 2020)

What happened

As France's oldest daily newspaper, Le Figaro has documented some of the country's most monumental events: the birth of the three separate republics, the rise of the Eiffel Tower, two world wars, the stardom and death of Albert Camus, and countless other milestones.

But Le Figaro made news of its own in April 2020 when a data leak exposed 7.4 billion user records of reporters, staff and subscribers. Security researchers say the breach stemmed from a misconfigured server operated by a vendor.[7] The vendor had left the data out in the open—lacking even basic password protection. The data was exposed for at least several months before an outside researcher discovered and reported it.

According to researchers, the compromised database also contained technical logs that exposed Le Figaro's backend servers and other potentially sensitive data. The information could be used for a wide range of attacks on Le Figaro's users, journalists, and employees.[8]

[7] Sergiu Gatlan *(BleepingComputer)*. "French daily Le Figaro database exposes users' personal info." May *2020.*

[8] *CISOMAG.* "French Newspaper Le Figaro Exposes 7.4 Bn Users' Records." May 2020.

Lessons learned

Many organizations rely on distributed workforces and extended supply chains, which help streamline business processes but complicate DLP. If a data breach is the fault of an outside vendor, your organization still gets the blame. That's why you must ensure that everyone in your supply chain is treating your data with the same level of care that you would.

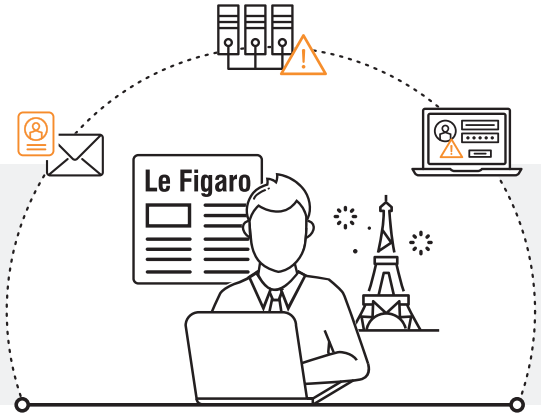
Attacks also may morph from data theft to more complex and dangerous attacks that target internal systems. Having early warning systems in place for such a contingency is key.

How to prevent it

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.

We recommend:

- Monitor the organization's infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) usage by insiders—employees and third-party contractors—to detect cloud server misuse early
- Ensuring that users from third-party vendors are monitored as they interact with your assets and data
- Making sure databases are properly configured
- Monitoring data activity to ensure that sensitive or regulated data is not leaving the environment



Attacks also may morph from data theft to more complex and dangerous attacks that target internal systems.

CONCLUSION AND NEXT STEPS

Every data loss incident is unique, but they all stem from people. That's why organizations must deploy a holistic security suite built for the way people work today.

By combining content-, behavior- and threat-based telemetry, you can address the full spectrum of data loss scenarios.

As these examples show, email, the cloud and endpoints are critical, interconnected pieces of the data loss puzzle. Users are constantly moving data between these channels. That means all three must be monitored and protected using a holistic approach with an integrated, unified solution.

Consider a solution that bridges all DLP channels that matter and:

- Addresses the full range of data risk from negligent, compromised and malicious users
- Saves time and administrative hassle by consolidating DLP policies across channels
- Enables faster response and investigations within security, compliance and other teams
- Provides a faster time to value than legacy DLP
- Enables compliance with data protection and privacy regulations across regions and within industries

To learn more about how a people-centric approach to DLP can help your organization better prioritize DLP activity, respond faster to incidents and achieve a shorter time to value, visit https://www.proofpoint.com/us/products/information-protection.

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. 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, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. **Proofpoint.com**

proofpoint.

0501-007-01-01 07/21