

WHITE PAPER

Your Next Data Breach Could Come from Someone You Trust

How insider risk exposes sensitive data across five industries, and three actions every business should take.

INSIDE THIS PAPER

- The scale of the problem: incidents and breaches by industry
- Insider-risk scenarios in banking, healthcare, manufacturing, retail and professional services
- The risk and the fix for each sector
- Three actions every business should take

INTRODUCTION

The threat already has access

A bank employee downloads customer records. A nurse uploads patient data to an AI tool. An engineer takes product designs to a competitor. Different industries, same problem: sensitive data is exposed by people who you trust that already have access.

You don't always need a sophisticated hacker to trigger a costly security breach. Sometimes, all it takes is excessive access, one careless click, or a security rule no one follows.

BY THE NUMBERS

How big is the problem?

The following figures come from Verizon's 2024 Data Breach Investigations Report, which analyzed thousands of real-world incidents. They are not all insider incidents.

Industry Sector	Reported Incidents	Confirmed Breaches	Primary Key Concern
Banking and Financial Services	3,348	1,115	Financial data and credentials
Healthcare	1,378	1,220	Patient data and misuse of access
Manufacturing	2,305	849	Intellectual property and operational systems
Retail and E-commerce	725	369	Payment data and customer credentials
Professional Services	2,599	1,314	Confidential client data and credentials

Source: Verizon 2024 Data Breach Investigations Report.

The insider-risk signal is especially strong in healthcare

On the following pages: where businesses are vulnerable, and what leaders can do about it.

BANKING & FINANCE

Protect customer & payment data

Role-based access, MFA and vendor reviews.



1 Banking and Financial Services

The problem: An employee downloads customer account data to a personal device, or a compromised vendor account accesses payment systems.

The risk: Fraud, customer data exposure, regulatory scrutiny, and lost trust.

The fix:

- Limit access to customer and payment data by job role.
- Flag unusual downloads and transfers.
- Require multifactor authentication and review vendor access regularly.

HEALTHCARE

Keep patient records private

Block unauthorized sharing and approve AI tools.



2 Healthcare

The problem: A staff member emails patient records to a personal account or enters patient information into an unapproved AI tool.

The risk: Patient privacy violations, legal exposure, and damaged trust.

The fix:

- Block unauthorized sharing of patient records.
- Approve AI tools before they handle sensitive data.
- Review access to patient records and train staff on safe data handling.

MANUFACTURING

Guard designs & production systems

Track bulk downloads, remove supplier access.



3 Manufacturing

The problem: An engineer copies product designs before joining a competitor, or a supplier retains access to production systems after a project ends.

The risk: Stolen trade secrets, competitive harm, and production disruption.

The fix:

- Restrict access to designs and production systems.
- Track bulk downloads and file transfers.
- Remove supplier access when projects end.

RETAIL & E-COMMERCE

Secure customer accounts

Individual logins, MFA and export alerts.



4 Retail and E-commerce

The problem: An employee exports customer data or shares login credentials with a coworker.

The risk: Data theft, fraud, and reputational damage.

The fix:

- Use individual accounts and multifactor authentication.
- Limit access to customer and payment data.
- Alert security teams to unusual data exports and account activity.

PROFESSIONAL SERVICES

Use AI without leaking client data

Approved tools, clear rules, trained staff.



5 Professional Services

The problem: An employee uploads confidential client files into a public AI tool to draft a report or presentation.

The risk: Loss of client confidentiality, contract violations, and damaged relationships.

The fix:

- Provide approved AI tools and clear usage rules.
- Prevent sensitive client data from being shared with unapproved tools.
- Train staff on confidentiality and monitor risky data transfers.

ACTION PLAN

Three actions every business should take

01

Know your data.

Identify your most sensitive information and where it lives.

02

Limit access.

Give employees and vendors only the access they need and remove it when they no longer need it.

03

Detect problems early.

Monitor unusual activity, train employees, and establish a clear incident response plan.

THE BOTTOM LINE

You can't eliminate every mistake or malicious act. But you can make sensitive data harder to misuse, catch problems sooner, and limit the damage when something goes wrong.



About IRSYS Corporation

IRSYS delivers end-to-end IT infrastructure, cyber security, cloud, consulting, and managed services, enabling secure operations, improved performance, and scalable growth.

Want to know where your insider risk is today? Talk to our team about access reviews, data protection and security monitoring for your business.

PHONE

630-588-2902

EMAIL

contactus@irsys.com

WEB

irsys.com

ADDRESS

450 W Schaumburg Road # 68025, Schaumburg, IL 60168