Sample data. Not a real company.

COMPANY EXPOSURE BRIEFING

October 20, 2026

example.com

60 people (estimate) *

F

EXPOSURE GRADE

38 company email accounts found in stolen data.

At least 1 includes enough personal data to open accounts in someone's name.

The one employee benefit that protects the business back.

Your people's data is already out there. Be the employer who protected them before, not the one who apologized after.

CHANCE SOMEONE IS HIT THIS YEAR

More than 9 in 10

Bureau of Justice Statistics: 9% of people a year

WHAT EACH CASE COSTS

$1,517 + 10–18 hours

Javelin 2026

COVER THE WHOLE TEAM

$14 per person per month

$10,080 a year. About 30% below the $19.99 individual price.

On these numbers, it pays for itself.

Prepared by Uncompromized

UNCOMPROMIZED

* Headcount provided by the requester.

FINDING #1 · STOLEN AND REUSED PASSWORDS

These are your people.

38 company email accounts at example.com are in stolen-login data. 24 with a password exposed.

Finance 3 | Leadership 3 | HR 4 | IT 2 | Staff 26 | Newest exposure August 2026 | 1 shared password

a•••••••s@example.com	password exposed (9 characters)	Collection #1, LinkedIn 2021
b•••••g@example.com	password exposed (9 characters)	Canva 2019
c••@example.com	password exposed (11 characters)	Dropbox 2012, Adobe 2013
o•••r@example.com	password exposed (8 characters)	Stealer log 2026
h•@example.com	password exposed (9 characters)	MyFitnessPal 2018
i•@example.com	password exposed (13 characters)	Stealer log 2026
j•••••@example.com	password exposed (9 characters)	Canva 2019
p••••••l@example.com		Twitter 2022
s••••0@example.com		LinkedIn 2021
s••••1@example.com		LinkedIn 2021

+28 **more of your people are in this data.**
We list 10 here.

Why this matters · *Every one of these is a working key someone can try against your email, banking and payroll, and most people reuse the same password at home. One reused password turns into a wire transfer to the wrong account. Your MSP resets them and turns on MFA. Monitoring is included for every employee, and each one turns it on themselves. If a stolen login leads to identity theft, the Recovery Concierge™ service does the recovery work.*

People reported $20.9 billion in cybercrime losses to the FBI in 2025, up 26% in one year. The real number is far higher: once unreported cases are counted, the FTC estimates fraud losses in a single year (2023) at $23.7 billion to $158.3 billion. (FBI IC3 2025 Internet Crime Report (1,008,597 complaints; $20.877B reported losses, up 26% from 2024); FTC, Protecting Older Consumers 2023–2024 (Oct 2024), p. 28: 2023 losses adjusted for underreporting estimated at $23.7B (conservative) to $158.3B)

About 60% of breaches involve a person: a click, a reused password, a convincing call. (Verizon 2025 Data Breach Investigations Report)

Attacks reach businesses through their people in 7 proven ways. We found 6 of them at example.com.

1	Stolen and reused passwords	Found at your company: 38 work logins, 24 with passwords
2	Password-stealing malware	Found at your company: 2 computers
3	Fake invoices and spoofed email	Found at your company: no email protection, 3 lookalike domains
4	Impersonating leaders and finance staff	Found at your company: 6 addresses exposed
5	Identity theft hitting employees	Found at your company: at least 1 account with identity data
6	Payroll, HR and vendor breaches	Found at your company: 1 vendor with breach reports
7	If your company is breached	Affects every business

1 Stolen and reused passwords

Found at your company: 38 work logins, 24 with passwords

How it reaches the business

Stolen logins are a leading way attackers get in: credential abuse started 22% of breaches, just ahead of exploited vulnerabilities at 20% (Verizon 2025 DBIR). People reuse passwords between work and home, so a leak from a shopping site can open company email.

Why each employee needs Uncompromized

Monitoring is included for every employee. Once they turn it on, they're alerted when their personal logins turn up in breach data. If a stolen login is used to steal their identity or money, the Recovery Concierge service does the recovery, with up to $1M in coverage.

What the business gets back

Employees who change an exposed password at home close the same door at work. And recovery happens without company time.

An MSP can

reset these logins and turn on MFA.

2 Password-stealing malware

Found at your company: 2 computers

How it reaches the business

Malware steals every saved login on a computer at once. 46% of infected systems holding company logins were unmanaged devices with both personal and work logins on them (Verizon 2025 DBIR). Nearly one-third of companies hit by ransomware had an earlier infostealer infection (SpyCloud 2025). Ransomware was part of 88% of breaches at small and mid-sized businesses (Verizon 2025 DBIR).

Why each employee needs Uncompromized

The same infection takes their personal banking and email logins. Covered employees get restoration and coverage, including stolen funds from personal accounts the bank won't return.

What the business gets back

Home computers are outside an MSP's reach. When the infection happens there, the employee still has specialists and coverage instead of handling it alone on company time.

An MSP can

clean affected machines and reset access.

3 Fake invoices and spoofed email

Found at your company: no email protection, 3 lookalike domains

How it reaches the business

Business email compromise cost US victims more than $3 billion in 2025 (FBI IC3 2025 Internet Crime Report). Spoofed addresses and lookalike domains make fake invoices look real.

Why each employee needs Uncompromized

UnVizible™ data broker removal takes employees' home addresses, phone numbers and family details off the sites attackers research them on. If a scam still costs them money or their identity, covered employees get lost wages, legal help and stolen-funds coverage.

What the business gets back

UnVizible is included for every employee, and each one turns it on themselves. Less personal detail online leaves attackers less to make a fake message convincing.

An MSP can

enforce email authentication and monitor lookalike domains.

4 Impersonating leaders and finance staff

Found at your company: 6 addresses exposed

How it reaches the business

Scammers buy detailed personal profiles from data brokers (CFPB, 2024). A home address, phone number and family names make a fake call from 'the owner' convincing, and personal details help criminals guess passwords and security answers (FBI IC3, 2025). Phone-number takeovers (SIM swaps) drew 971 complaints and $17.4 million in losses in 2025 (FBI IC3 2025 Internet Crime Report).

Why each employee needs Uncompromized

UnVizible™ data broker removal is included for every employee and takes their personal listings off data broker sites. If their identity is still stolen, the Recovery Concierge service does the recovery.

What the business gets back

Leaders and bookkeepers who are harder to research are harder to impersonate.

An MSP can

help set up call-back verification for payment and banking changes.

5 Identity theft hitting employees

Found at your company: at least 1 account with identity data

How it reaches the business

Identity theft takes a victim 10 to 18 hours to resolve (Javelin 2026 Identity Fraud Study), much of it during work hours. 1 in 10 identity theft victims lost at least $10,000 (Identity Theft Resource Center, 2023 Consumer Impact Report).

Why each employee needs Uncompromized

The Recovery Concierge service does the recovery. Coverage up to $1M with a $0 deductible, including lost wages of $1,000 a week for up to 5 weeks.

What the business gets back

Employees stay focused on their jobs instead of on hold with banks and credit bureaus.

6 Payroll, HR and vendor breaches

Found at your company: 1 vendor with breach reports

How it reaches the business

Breaches involving a third party doubled to 30% (Verizon 2025 DBIR). Payroll, HR and benefits providers hold employees' Social Security numbers and bank details.

Why each employee needs Uncompromized

Coverage and restoration apply no matter which company leaked their data.

What the business gets back

When a vendor is breached, your people already have help, and nothing on your own network could have stopped it anyway.

An MSP can

review which vendors hold employee data.

7 If your company is breached

Affects every business

How it reaches the business

A breach of 4,060 employee and customer records would cost about $649,600 ($160 per record, IBM Cost of a Data Breach 2025 global average for customer personal data; employee records average $168, so this is the lower figure). Companies are expected, and in some states required, to offer identity protection after a breach (Connecticut requires at least 24 months when Social Security or taxpayer ID numbers are exposed, Conn. Gen. Stat. § 36a-701b).

Why each employee needs Uncompromized

Already enrolled, with restoration and coverage in place before anything happens.

What the business gets back

One less thing to buy in the middle of a crisis.

An MSP can

protect the systems so this is less likely to happen.

Your MSP protects the systems. Uncompromized protects the people.

UnVizible™ takes your people off the shelf.

UnVizible covers 440 data brokers and removes your employees' personal information (home addresses, phone numbers and family details) from 432 of them automatically, including Spokeo, Whitepages, BeenVerified, LexisNexis and Acxiom. Your employees don't fill out a single opt-out form.

Attackers shop for your people on data broker sites. Fewer listings means less to build a fake invoice, an impersonation call or a phishing email from.

Broker coverage as of August 2026.

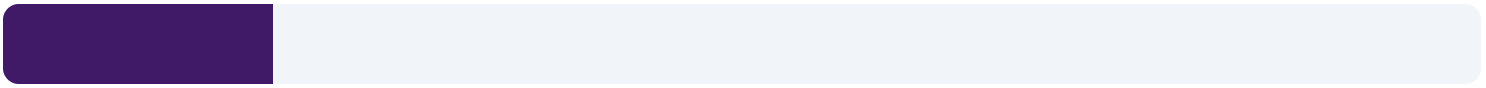
Your choice, per year

No coverage **$32K–$66K**



$0 coverage + $22,755–$51,450 employee losses + $9,720–$14,715 lost work.

Uncompromized **$12K**



60 × $14/month × 12 = $10,080 + 15 cases × 3 hours (estimate) × $45 = $2,025.

Total yearly cost for about 60 people (estimated): coverage plus the losses you still carry. Solid = low estimate, shaded = high.

Who does the work?

~~Your employee, on the phone for 10–18 hours~~

The Recovery Concierge service does the work

Worst case for one person?

~~Uncapped~~

Up to $1M, $0 deductible

Lost wages and legal help?

~~Out of pocket~~

Up to $5,000 wages, legal defense, stolen funds

A BAD YEAR

1 in 10 identity theft victims lost at least $10,000.

Uncompromized: **up to $1,000,000**, $0 deductible

This is a share of victims, not a forecast for your company. Applies to the about 15 people likely hit this year (see the math above).

Source: Identity Theft Resource Center, 2023 Consumer Impact Report

COVERAGE PER DOLLAR

$5,952 of coverage per $1

Uncompromized: $1,000,000 ÷ $168 a year

> **An alert tells you something happened. Restoration makes it un-happen.**
>
> Ask what happens if it goes wrong: how much is covered, and who does the work.

Uncompromized protects the people. Your MSP protects the systems.

Cyber insurance readiness

Questions that commonly appear on cyber insurance applications, and what can be seen from outside the company. This is about readiness, not how any insurer will decide.

Is email authentication (SPF and DMARC) in place? No DMARC policy is published.	Likely to come up
Is remote access kept off the open internet? 1 system shows remote access open to the internet.	Likely to come up
Is MFA on for remote access and email? MFA can't be verified externally. Your MSP can confirm it.	Can't tell from outside
Any malware-infected machines? 2 staff computers show password-stealing malware.	Likely to come up
Any known breaches or leaked credentials? 1 known breach, 38 leaked accounts.	Likely to come up

The details

The math, sources and full findings behind every number above.

Based on 60 employees (your estimate), 4,000 customer records (estimated) and $45/hour staff cost (BLS average). Grade F, exposure score 0/100.

Estimated yearly exposure for your people

$32,475 – $66,165

About 15 people likely hit this year (from an estimated headcount): 38 exposed people × 1 in 3, plus 22 others × the 9% national yearly rate.

How it adds up: 15 people likely hit (38 exposed people × 1 in 3, plus 22 others × the 9% national yearly rate) × $1,517–$3,430 loss each (Javelin 2026; BJS), plus 15 × 10.4–17.8 hours to resolve (Javelin 2026) + 4 HR hours (estimate) × $45/hour (BLS, rounded down). = $22,755–$51,450 + $9,720–$14,715.

What it costs each employee

$22,755 – $51,450

15 people likely hit this year (38 exposed people × 1 in 3, plus 22 others × the 9% national yearly rate) × $1,517 average loss (calculated from Javelin's published totals), up to $3,430 when a new account is opened in their name. 1 exposed account includes the personal data a new account needs

What the member policy pays for: The Recovery Concierge service, with specialists who do the recovery work; Lost wages, $1,000 a week for up to 5 weeks; Legal defense for creditor suits and removing wrongful judgments (criminal defense only after acquittal or dropped charges); Unauthorized electronic transfers from personal accounts the bank hasn't reimbursed; Recovery costs: re-filing credit applications, notary, phone and postage, up to six credit reports. Up to $1M, $0 deductible.

Source: Calculated from Javelin Strategy & Research, 2026 Identity Fraud Study published totals ($27.3B in 2025 identity fraud losses across 18M victims); Bureau of Justice Statistics, Victims of Identity Theft (2021 data, pub. 2023); Javelin Strategy & Research, 2014 Identity Fraud Study (1 in 3 people notified of a data breach in 2013 became identity fraud victims; Javelin's most recent measurement of this figure)

What it costs the company in lost work

$9,720 – $14,715

15 people × 10.4–17.8 hours to resolve + 4 hours of HR and manager time (estimate) × $45/hour

Uncompromized reduces this: the Recovery Concierge service does the recovery work, so covered employees get back to work, and it's a benefit they notice.

Source: Javelin Strategy & Research, 2026 Identity Fraud Study; BLS Employer Costs for Employee Compensation, September 2025 (private industry total compensation $46.05/hour, rounded down to $45)

If the company itself is breached

$649,600 – $1,624,000

4,060 employee and customer records × $160 per record, up to 2.5× with lawsuits and fines. The average US breach costs $10.22M.

Not covered by identity protection. That's your MSP's work. After a breach, companies are expected, and in some states required (Connecticut: 24 months when SSNs are exposed), to offer identity protection. With Uncompromized, your employees would already have it.

Source: IBM Cost of a Data Breach Report 2025 (U.S. average breach $10.22M; global average $160 per customer personal-data record)

Your options, per year

	No coverage	Uncompromized · $14/employee
Coverage cost	$0	**$10,080**
Who does the recovery	The employee, alone	**The Recovery Concierge service does the work**
Employee hours per case	10.4–17.8	**A few, with the work handled for them***
Lost work per case	$648–$981	**Mostly removed; lost wages paid up to $5,000**
Worst case for one person	Uncapped	**Covered up to $1M, $0 deductible**
Legal defense and stolen funds	Out of pocket	**Included, within the $1M**
After a company breach	Buy protection for everyone	**Covered employees already protected**
Expected yearly cost (an average year)	**$32,475 – $66,165**	**$12,105**
How each total adds up	$0 coverage + $22,755–$51,450 employee losses + $9,720–$14,715 lost work.	60 × $14/month × 12 = $10,080 + 15 cases × 3 hours (estimate) × $45 = $2,025.

Uncompromized total includes about 3 hours per case of employee and HR time. *Estimate. HR and manager time (4 hours per case) is an estimate. Coverage from the identity theft protection policy issued to every member: $1,000,000 aggregate limit per policy period, $0 deductible; legal costs count within the $1M, not in addition to it. Lost wages are a sublimit. Personal accounts and identity only; business or commercial accounts and business identity are excluded. The member must report within 90 days of discovery, and the event must first be discovered while enrolled.

At least 1 of 38 exposed accounts includes identity data, enough to open accounts in someone's name.

7
Login only (accounts)
Email and password. Your MSP's work: reset and MFA.

2
Contact details (accounts)
Name, phone, city. Fuel for convincing scams.

1
Identity data (account)
Birth date, home address or ID. What new-account fraud needs. What restoration and coverage are for.

Based on the 10 accounts with detailed records out of 38 found. "None found" means none in these sources, not that none exists.

Your vendors

Example Payroll Co. entered

Appeared in a breach report: Maryland Attorney General, 2025-02-11 (4,210 people).

Example HR Cloud found in DNS

No breach report found in the sources we check.

Why this matters · *Payroll and HR providers hold your employees' Social Security numbers, birth dates and bank details. When one of them reports a breach, your employees' data may be included, and nothing on your own network could have stopped it. If it's used against a covered employee, they get restoration and coverage.*

Malware-Stolen Logins

2

staff computers infected by password-stealing malware · plus 14 customer logins stolen

Most recent staff infection: Aug 19, 2026

Why this matters · *Malware on a staff computer copies every saved login on it — banking, payroll, remote access. Whoever holds them can move company money while looking exactly like your employee, and the same file holds that person's personal accounts. Nearly one-third of companies hit by ransomware had an earlier infostealer infection (SpyCloud). Your MSP cleans the machine and resets access. If the employee's own identity is misused, a covered employee gets the Recovery Concierge service and up to $1M in coverage.*

Email Spoofing Risk

High

Anyone can send email that looks like it came from them

SPF soft | DMARC missing | DKIM not found | Microsoft 365

Why this matters · *A forged invoice from your own address is how payment fraud starts, and that money almost never comes back. Your customers get the fake too, so you carry the loss and the reputation. Your MSP tightens the domain. If staff are targeted personally and it costs them, covered employees get lost wages, legal help and stolen-funds coverage.*

Lookalike Domains

3

lookalike domains are live · 2 can receive email

examp1e.com · takes email · since Jul 2, 2026
example-billing.com · takes email · since May 14, 2026
exarnple.com · since Nov 30, 2025

Why this matters · *A near-copy of your name is registered and live. Customers pay the wrong invoice, and you refund the money and explain it. Staff get the same trick on personal accounts, which is how attackers get their credentials in the first place.*

Breaches of the Company

1

known breach of the company itself

Example.com customer portal · Mar 11, 2024

Why this matters · *Your customers' data is already circulating, which drives claims, churn and hard conversations. Your own employees are inside the same file, and covered employees get the Recovery Concierge service, not just a notice.*

Exposed Systems

1

company system with risky services open to the internet · 1 vulnerability actively used by attackers

`remote.example.com` · Remote desktop (RDP) · **CVE-2019-0708 actively used by attackers**

Why this matters · *An open remote desktop or file share is a front door attackers try every day, and a known, exploited vulnerability is one they already have the key for. Your MSP closes these. Uncompromized protects the people.*

What's included for every employee

The employee benefit built to protect the business: UnVizible data broker removal included for every employee, the Recovery Concierge service doing the recovery work, and everything built, hosted and supported in the USA.

A leading standalone data removal service costs $10.75 a month on its own, billed yearly, with no identity-theft protection. For $14 a month per employee, Uncompromized includes UnVizible data broker removal, the Recovery Concierge service, up to $1M in identity theft coverage, and monitoring — all built, hosted and supported in the USA.

Source: A leading standalone data removal service, 1-person annual plan, $129 a year (published price, October 2026); data removal only, no identity-theft protection.

PREVENTION

- UnVizible™ data broker removal (440 brokers tracked, 432 removed automatically, as of August 2026). Each employee turns it on themselves.
- Monitoring, included for every employee.

PROTECTION

- Up to $1M identity theft coverage, $0 deductible.
- Lost wages, $1,000 a week for up to 5 weeks.
- Legal defense for creditor suits and wrongful judgments.
- Unauthorized transfers from personal accounts the bank won't return.
- Recovery costs.

RECOVERY

- The Recovery Concierge™ service does the recovery work for the employee.

Built, hosted, developed and supported entirely in the USA.

Your MSP doesn't just resell Uncompromized. They help build it.

We work with our MSP partners every day to make Uncompromized better, based on what they see protecting businesses like yours.

What happens next

1 **Review these findings with your IT provider.**

The system fixes become their quote.

2 **Cover your team: $14 per employee per month.**

One enrollment link for the whole team.

https://uncompromized.com

3 **Your employees activate.**

Monitoring and data removal are included; each person turns them on themselves.

Sources: Javelin Strategy & Research, 2026 Identity Fraud Study; Javelin Strategy & Research, 2014 Identity Fraud Study (1 in 3 people notified of a data breach in 2013 became identity fraud victims; Javelin's most recent measurement of this figure); Bureau of Justice Statistics, Victims of Identity Theft (2021 data, pub. 2023); Identity Theft Resource Center, 2023 Consumer Impact Report; SpyCloud 2025 Identity Exposure Report; IBM Cost of a Data Breach Report 2025 (U.S. average breach $10.22M; global average $160 per customer personal-data record); BLS Employer Costs for Employee Compensation, September 2025 (private industry total compensation $46.05/hour, rounded down to $45); Shodan InternetDB (public, passive; no scanning performed); CISA Known Exploited Vulnerabilities catalog; A leading standalone data removal service, 1-person annual plan, $129 a year (published price, October 2026); data removal only, no identity-theft protection; UnVizible broker coverage, as of August 2026.