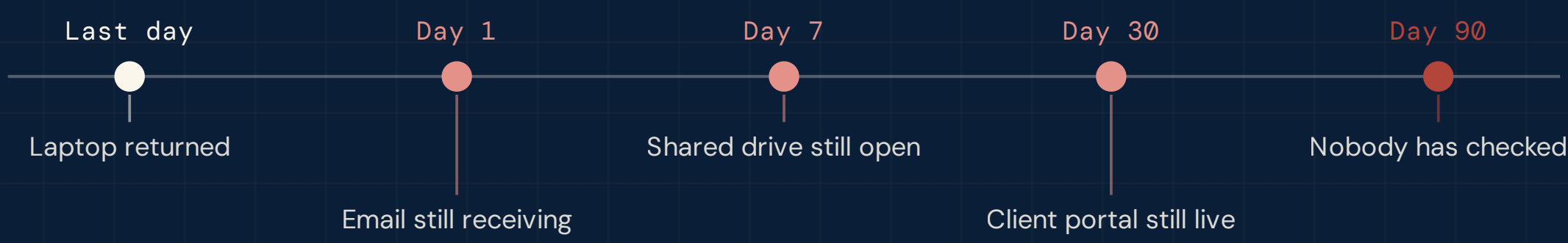
A SHORT BRIEF FOR FOUNDERS AND AGENCY OWNERS

The Access Gap

The people who left still have accounts. Attackers do not check your headcount before they knock. And the statistic everyone quotes about this was disavowed by the people who published it.

WHAT HAPPENS AFTER SOMEBODY LEAVES

Nobody decides to leave the door open. Closing it was simply never assigned to anyone.



Stolen credentials were the most common way into a breach.

An account nobody closed is a credential nobody has to steal.

The fix is a list, a named owner and a same-day rule.

No software required. This is operations work, not security work.

88 percent of small business breaches involve ransomware, against 39 percent at large firms.

Verizon Data Breach Investigations Report 2025

Paul Prado Pacardo

Senior Executive Assistant · Operations and Project Manager

me.kabuhayan.app
linkedin.com/in/paulpacardo
pacardopaul18@gmail.com

THE FINDING THAT INVERTS THE ASSUMPTION

Small businesses face a harder profile than large ones.

Not a smaller version of the same threat. A different and more punishing mix, from real incident data rather than a survey of what owners fear.

88%

of small and medium business breaches involve ransomware

Verizon DBIR 2025

39%

the equivalent share at large enterprises

Verizon DBIR 2025

22%

of breaches began with stolen credentials, the single most common entry point

Verizon DBIR 2025

THE METHOD

22,052 incidents and 12,195 confirmed breaches across 139 countries

Verizon's annual report aggregates real incident data contributed by dozens of organisations. It counts what happened, not what people believe might happen. That distinction matters enormously in this field.

WHY THE GAP

Attackers automate, and automation does not check your headcount

Scanning for exposed credentials and unpatched systems costs the same whether you have eight staff or eight thousand. Small firms are not being singled out. They are simply the ones with the weakest controls when the automated sweep arrives.

ALSO

The human element featured in around 60 percent of breaches

Which is not an argument for more training videos. It is an argument for removing the situations where a single human mistake is enough on its own.

SAY IT PLAINLY

You are not too small to be a target. On this particular measure, you are the easier one.

WHERE THE DOOR IS ACTUALLY LEFT OPEN

The laptop came back. The accounts did not.

Nobody decides to leave a former employee with live access. The physical handover has an obvious owner and an obvious deadline. The digital one has neither.

What reliably comes back

Laptop, phone, building pass, keys. Tangible, countable, and somebody notices if they are missing. There is a person whose job it is to collect them and a day on which it happens.

What reliably does not

Email forwarding, shared drive access, the client portal login, the password manager vault, the third-party tools bought on a card, the shared account whose password never changed.

THE PATTERN

Access is granted one tool at a time and revoked all at once, or not at all

Every new tool adds an account. Nobody keeps the list, because keeping the list was never assigned. On the last day there is nothing to work from, so the offboarding is done from memory.

THE MULTIPLIER

Shared logins survive every departure

A password four people know does not get revoked when one leaves. It gets remembered. Shared accounts are the single most common reason access outlives employment in a small business.

THE HONEST BIT

Almost nobody leaves intending to misuse it

The risk is rarely a vengeful former employee. It is a live credential sitting in an old password manager on a personal laptop, waiting to be part of somebody else's automated sweep.

THE SENTENCE THAT MATTERS

An account nobody closed is a credential nobody has to steal.

THE STATISTIC I AM REFUSING TO USE

Sixty percent of small businesses do not close after an attack.

You have read that they do. It is the most quoted cyber statistic aimed at small business, it appears in sales decks and government pages, and the organisation credited with it has publicly disowned it.

What happened to it

In May 2022 the National Cyber Security Alliance stated plainly that the figure was a third-party 2011 statistic, that it was not generated from their research, that they could not verify its original source, and that they do not recommend its ongoing use. They removed it from their site.

And the usual replacement

The fallback figures, that around 19 percent of small businesses would face bankruptcy or 40 percent would close after a large attack, are widely attributed to Verizon. They are not Verizon's. They come from a security vendor's survey of roughly 200 owners, asked what they imagine would happen.

WHY IT MATTERS

Fear is a poor basis for an operational decision

A number designed to frighten you into a purchase is not a number you should plan around. If the honest figures were not alarming enough, that would be worth knowing too. They are.

WHAT I USE

Verizon for incidents, IBM with Ponemon for cost, Hiscox for small-business impact

Named studies, stated methods, and in Verizon's case real incident records rather than recalled opinions. Where a source is an insurer or a vendor I say so on the page.

THE STANDARD, AGAIN

A brief that quotes a number it cannot trace is a brief you should not act on. That applies to this one as much as to anybody else's.

WHAT IT ACTUALLY COSTS, HONESTLY

Not millions. Still more than you have spare.

The enterprise figures you see quoted are real and irrelevant to you. Here are the ones measured on businesses your size.

~$8,300

median cyberattack cost for a US small business

Hiscox Cyber Readiness Report 2023

41%

of small businesses reported being attacked in that year

Hiscox, 2023

38%

of small businesses have nobody at all assigned to security, and 42 percent have exactly one person

DigitalOcean Currents, 2023

READ IT RIGHT

The median is not the risk

Most incidents are survivable and unremarkable. The distribution has a long tail, and the tail is where a business gets hurt. A median of $8,300 does not mean your worst case is $8,300.

THE REAL COST

Downtime and the client conversation usually exceed the ransom

Ransomware incidents commonly run to weeks of disrupted operation. For a service business the expensive part is explaining it to clients whose data you hold, not the payment itself.

SOURCE NOTE

Hiscox sells cyber insurance

Their method is transparent, the fielding was done by Forrester, and the sample includes over 500 US small businesses. Both facts are true and you should hold them together.

THE FIGURE THAT EXPLAINS ALL THE OTHERS

Nearly four in five small businesses have one person or nobody responsible for this. Not a small security team. One person, or no one.

WHAT ACTUALLY CLOSES THE GAP

A list, an owner, and a same-day rule.

None of this requires software, a consultant, or a security budget. It requires somebody to be responsible for it, which is the part that is usually missing.

STEP 01

Write the access list first

Every tool, account and shared login the business uses, and who has access to each. Build it once, from the card statement and the tool list rather than from memory. Most owners find at least one subscription nobody could name.

STEP 02

Attach it to the leaving process

The offboarding checklist already exists for the laptop and the final payslip. Access revocation goes on the same list, with the same owner and the same deadline. It is an operations item, not an IT project.

STEP 03

Revoke on the last day, not the last week

Same day, every time, including for people leaving on good terms. A rule with exceptions is a preference, and preferences are what leave accounts open for ninety days.

> **Turn on multi-factor authentication and kill shared logins before you buy anything at all.**
>
> Stolen credentials were the most common way into a breach. Both of those measures directly attack that route, and both are free.

WHY THIS NEVER GETS DONE

It is nobody's job, it is not urgent until it is catastrophic, and it produces nothing anyone can see. Which is exactly the category of work that needs an owner rather than good intentions.

EVIDENCE, NOT ADJECTIVES

This is the kind of list I have actually kept.

Access administration, onboarding and offboarding are executive assistant and operations work, and they are the work I have done across multiple businesses.

MAINTAINED

Accounts and tool access

Maintaining project and client records across CRM platforms and project tools, managing account profiles and listings across digital platforms, and the vendor relationships behind them.

DOCUMENTED

Standard operating procedures

Developing and implementing SOPs for recurring administrative workflows, which is exactly the mechanism an offboarding checklist lives inside.

CONTROLLED

Internal controls experience

Helped implement internal controls that reduced fraud risk and supported regulatory compliance, and managed compliance requirements across a project lifecycle in financial services.

AUTOMATION	**40+ automation rules and scripted jobs, including scheduled checks and escalations** The same mechanism that chases an overdue ticket will chase an unrevoked account. Escalation on a rule rather than on somebody remembering is the whole point.
COMPLIANCE	**Five years working under KYC, AML, BSA and GLBA requirements** Including data confidentiality standards and business continuity planning. Access discipline is not a new idea to me, it is where I started.
CREDENTIALS	**Google Project Management Professional Certificate and Google AI Essentials** Plus Anthropic AI Fluency and Model Context Protocol. 31 certifications in total, every one independently verifiable.

WHAT I AM NOT

I am not a security engineer and I will not pretend to be one. This brief is about the operational half, which is where most small-business exposure actually lives.

HOW TO START

Name the last person who left. Then check.

You do not need an audit to begin. You need one former employee and twenty minutes, and the result will tell you whether the rest of this applies to you.

OPTION 01

Check one leaver

Take the most recent departure and try their email, the shared drive, and one client tool. Twenty minutes. Whatever is still live tells you what the process actually does, rather than what you believe it does.

OPTION 02

Let me build the list

Every tool, account and shared login, who holds access, and an offboarding checklist attached to the leaving process with a named owner and a same-day rule. A few days, and it does not expire.

OPTION 03

Do the two free things

Turn on multi-factor authentication everywhere it is available, and end shared logins. Both attack the most common entry route directly, and neither costs anything but an afternoon.

WHAT I WOULD EXPECT YOU TO FIND

At least one active account belonging to someone who has left. One subscription nobody can identify. And a shared password that has not changed since before the last two departures.

Available now for remote work

Chief of Staff · Operations · Senior Executive Assistant · Project Manager

Check one leaver and tell me what was still open. I will tell you where I would start.

pacardopaul18@gmail.com
linkedin.com/in/paulpacardo
me.kabuhayan.app

Sources: Verizon Data Breach Investigations Report 2025; 22,052 incidents and 12,195 confirmed breaches across 139 countries, November 2023 to October 2024. Hiscox Cyber Readiness Report 2023, fielded by Forrester Consulting; 5,005 professionals across eight countries including over 500 US small businesses; Hiscox sells cyber insurance. DigitalOcean Currents Cybersecurity report 2023; survey of over 550 small business founders and executives. Deliberately excluded: the claim that 60 percent of small businesses close within six months of a cyberattack, publicly disavowed by the National Cyber Security Alliance in May 2022 as an unverifiable third-party 2011 figure; and the commonly repeated bankruptcy and closure percentages misattributed to Verizon, which originate from a security vendor survey of approximately 200 owners. Figures are third-party research, not results I am claiming.