SUPPORT BAY, LLC · LOS ANGELES SINCE 1988

WHITE PAPER

7 cybersecurity basics every small business needs

What the latest breach research says about how attacks really happen, and the practical controls that stop most of them.

Who it's for
Owners and managers of 1–100 person teams

Time to read
About 12 minutes

Published
November 2026

EXECUTIVE SUMMARY

Most breaches start with something ordinary

Attackers rarely need anything exotic. They use a reused password, an unpatched device, a convincing email or a vendor's access.

Verizon's 2026 Data Breach Investigations Report analyzed more than 22,000 confirmed breaches. It found people were involved in most of them, ransomware appeared in nearly half, and small organizations are disproportionately affected by ransomware.[1] The good news is that the controls that stop the most common attacks are well understood and affordable for a small business.

62%
of breaches involved the human element: errors, misuse, stolen credentials or social engineering.
Verizon 2026 DBIR[1]

48%
of breaches involved ransomware, up from 44% the year before.
Verizon 2026 DBIR[1]

$4.99M
global average cost of a data breach in 2026.
IBM Cost of a Data Breach 2026[2]

31%
of breaches began with an attacker exploiting a software vulnerability.
Verizon 2026 DBIR[1]

48%
of breaches involved a third party such as a vendor or partner.
Verizon 2026 DBIR[1]

~$3B
in business email compromise losses reported to the FBI in 2025.
FBI IC3 2025, via SecurityWeek[3]

MYTHS THAT LEAVE BUSINESSES EXPOSED

Four things we hear, and why they don't hold up

“We're too small to be a target.”
Most attacks are automated and opportunistic. Verizon reports that small organizations are disproportionately hit by ransomware.[1]

“Microsoft backs up our email.”
Cloud providers keep their service running, but protecting and restoring your data is largely your responsibility. A separate backup is what lets you recover.

“We have cyber insurance.”
Insurance helps with costs but doesn't prevent an attack, and insurers increasingly require controls such as MFA and backups before they will cover you.

“We're compliant, so we're secure.”
Compliance sets a minimum. Attackers target what is actually configured, patched and monitored today.

THE BASICS

Seven controls that stop most common attacks

1 Multi-factor authentication on every account

Stolen or guessed passwords remain a common way in. MFA means a password alone is not enough to sign in.

> **Do this:** Turn on MFA for email, Microsoft 365 or Google Workspace, remote access, banking and every admin account. Prefer authenticator apps or security keys over text messages.

2 Patch quickly, and retire unsupported equipment

Exploiting a known vulnerability was the starting point for 31% of breaches in Verizon's 2026 data.[1] Firewalls, VPNs and other internet-facing devices are favorite targets.

> **Do this:** Apply critical updates within days, not months. Replace any device or software that no longer receives security updates from its manufacturer.

3 Endpoint detection and response, watched around the clock

Traditional antivirus looks for known threats. Endpoint detection and response (EDR) watches for suspicious behavior and can isolate a device before an attack spreads. IBM found organizations using security AI and automation cut breach costs by almost $2 million on average.[2]

> **Do this:** Put EDR on every computer and server, and make sure someone is responding to its alerts 24/7, not just collecting them.

4 Email security and a payment-verification rule

Business email compromise, where criminals impersonate a boss, vendor or client to redirect a payment, cost businesses about $3 billion in FBI-reported losses in 2025.[3]

> **Do this:** Add advanced email filtering and protect your domain against spoofing (SPF, DKIM and DMARC). Make it a firm rule to confirm any new or changed payment details by calling a known phone number.

5 Backups you have actually tested

Ransomware was involved in 48% of breaches.[1] A clean, recent backup is what lets you recover without paying, and 69% of ransomware victims in Verizon's data did not pay.[1]

> **Do this:** Back up servers, computers and cloud data such as Microsoft 365. Keep at least one copy offline or unchangeable, and test a full restore at least twice a year.

6 Security awareness training that continues

With people involved in 62% of breaches, staff are both the most targeted and the most valuable line of defense.[1]

> **Do this:** Train everyone when they join and at least once a year, run regular phishing simulations, and make it easy and blame-free to report a suspicious message.

7 Control vendor access and plan for the worst day

Third parties were involved in 48% of breaches.[1] Every vendor with remote access, shared passwords or a connection to your systems extends your risk.

> **Do this:** Give vendors only the access they need, remove it when the work ends, and keep a one-page incident response plan: who to call, how to isolate systems and how to reach your insurer.

SELF-ASSESSMENT

How does your business measure up?

Tick each statement that is true today. Anything left blank is a priority.

	Statement
☐	Every user and admin account requires multi-factor authentication.
☐	Critical security updates are installed within 14 days, and nothing we use is past end of support.
☐	Every computer and server runs EDR, and someone responds to alerts 24/7.
☐	Our email has advanced filtering, and our domain uses SPF, DKIM and DMARC.
☐	Changes to payment instructions are always confirmed by phone.
☐	Our data, including Microsoft 365 or Google Workspace, is backed up, with one copy offline, and a restore was tested in the last six months.
☐	Everyone completes security training at least once a year, and we run phishing simulations.
☐	We know which vendors can access our systems, and access is removed when work ends.
☐	We have a written incident response plan and know who to call.

8–9 ticks: a strong foundation; focus on testing and monitoring. **5–7:** real gaps that attackers routinely use. **4 or fewer:** act now, starting with MFA, backups and EDR.

If you suspect an attack: the first hour

1. Disconnect affected computers from the network, but don't power them off.
2. Call your IT or security provider, then your cyber insurer.
3. Change passwords for affected accounts from a clean device.
4. If money was sent, contact your bank immediately and file a report at ic3.gov.
5. Write down what happened and when. Don't delete evidence.

Get a free cybersecurity assessment from Support Bay

Support Bay has helped Los Angeles businesses run and protect their technology since 1988. Our managed IT and cybersecurity team will review your current protection against these seven basics, explain the gaps in plain English and recommend a practical plan that fits your budget.

Call 310.294.8969 · supportbay.com

Sources

1. Verizon Business, “2026 Data Breach Investigations Report: Executive Summary,” 2026. verizon.com/dbir
2. IBM, “Cost of a Data Breach Report 2026,” and IBM Newsroom, July 29, 2026. ibm.com/reports/data-breach
3. FBI Internet Crime Complaint Center, “2025 Internet Crime Report,” as reported by SecurityWeek, April 2026. securityweek.com/fbi-cybercrime-losses-neared-21-billion-in-2025

This white paper is general information, not legal advice. Support Bay, LLC is a Los Angeles technology company founded in 1988 and the parent of SupportMax and Telling Marketing.