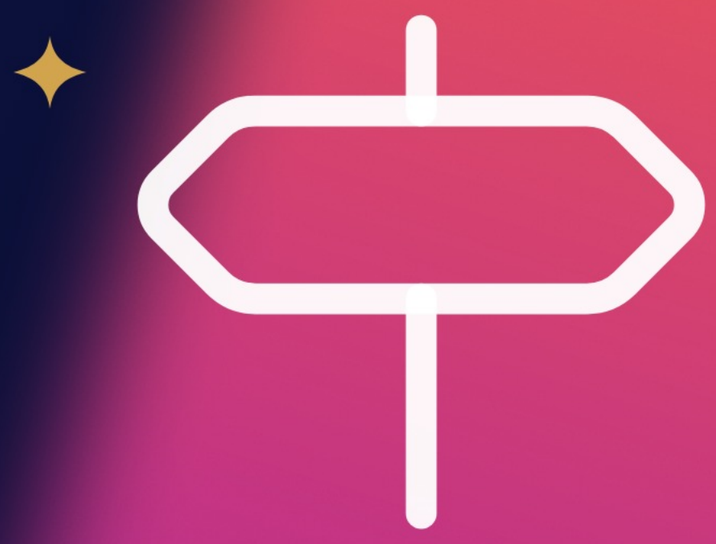
SOLUTION BUILDERS®

CYBERSECURITY AWARENESS MONTH 2026



PART 2 OF 3

The Alternatives.

Every business has a cyber risk strategy, even if that strategy is hoping. Here are the five most common, and what the data says about each.

5
common ways businesses try to handle cyber risk

78%
cut security staffing in half on weekends and holidays

31%
higher breach cost when containment drags past 200 days

01 The Problem

02 The Alternatives

03 The Solution

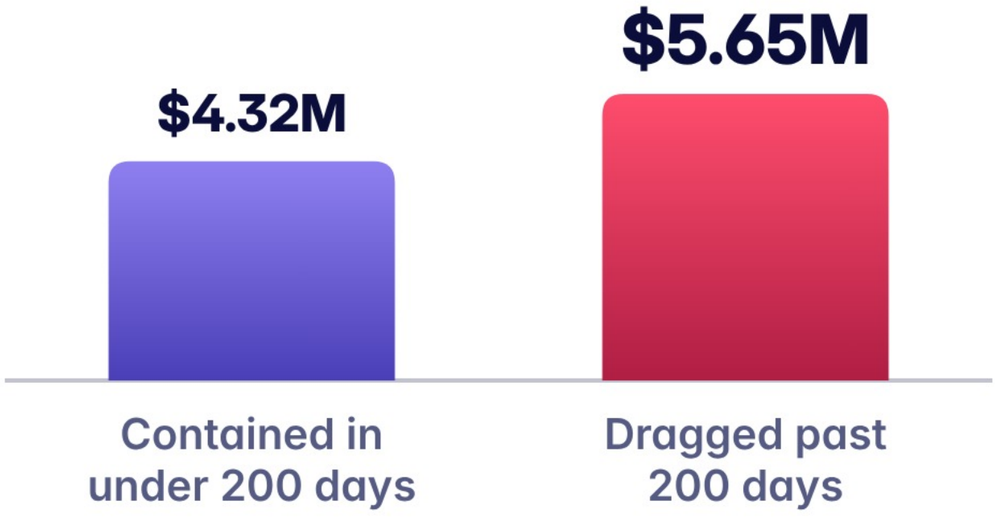
OPTIONS 1 AND 2

Hope is free. Right up until it is not.

OPTION 01

Do nothing and hope

"We are too small to be a target."



+31%

The longer a breach goes unnoticed, the more it costs. With nobody watching, nobody notices.

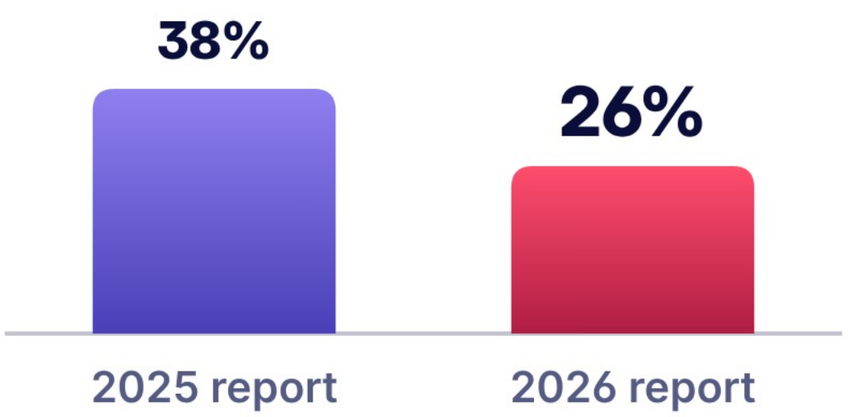
The verdict: the cheapest plan today and the most expensive one later.

OPTION 02

Buy some tools and call it done

"We have antivirus and a firewall."

CRITICAL KNOWN FLAWS FULLY PATCHED



53%

of breached organizations had not encrypted their sensitive data

Tools throw alerts. Somebody still has to read them, patch, and act.

The verdict: tools without people are just very expensive alarm clocks.

Sources: IBM Cost of a Data Breach Report 2026. Verizon Data Breach Investigations Report 2026.

OPTIONS 3 AND 4

A lot to ask of one person, or one policy.

OPTION 03

Leave it all to one IT person

"Our IT person handles it."



of companies cut security staffing by half or more on weekends and holidays

And **52%** of organizations surveyed were hit by ransomware on a weekend or a holiday. Attackers read calendars too.

The verdict: great people still need to sleep. Threats do not.

OPTION 04

Count on cyber insurance

"We are covered if something happens."

$139,875
median ransom payment in 2026

69%
of victims refused to pay and still had to recover

247
days to find and contain a breach, policy or no policy

The verdict: insurance pays a claim. It does not stop the attack or win back a client.

Sources: Semperis Ransomware Holiday Risk Report 2025. Verizon DBIR 2026. IBM Cost of a Data Breach Report 2026.

SIDE BY SIDE

Five options. Only one checks every box.

YOUR OPTIONS	STOPS ATTACKS EARLY	WATCHES 24/7	RESPONDS IN MINUTES	RECOVERS YOUR DATA	PREDICTABLE COST
Do nothing and hope	✗	✗	✗	✗	✗
Tools only	–	✗	✗	–	✓
One IT person	–	✗	–	–	✓
Insurance only	✗	✗	✗	–	–
Managed security partner	✓	✓	✓	✓	✓

● Yes ● Partly ● No

Our read of the options, based on the data in this series.

OPTION 05

A managed, layered security partner

People, process, and tools working together around the clock, for one predictable monthly cost.

$1.93M

lower average breach cost for organizations that use security AI and automation extensively

65 days

faster to find and contain a breach with those same capabilities

Source: IBM Cost of a Data Breach Report 2026.

BEFORE YOU PICK ONE

Five questions worth asking your team this week.

You do not need a consultant to start. You need honest answers to these.

1 If ransomware hit at 2 a.m. on a Saturday, who would know?

2 When did we last restore from a backup, for real?

3 Which accounts still do not have MFA turned on?

4 How long do critical patches actually take to get installed?

5 Are we really doing everything our insurance application says we do?

If any answer was **“I am not sure,”** that is your starting point. Part 3 shows what a real fix looks like.

NEXT UP · PART 3, THE SOLUTION →