VIKINGCLOUD®

BUSINESS UNINTERRUPTED.

A Vancouver
Sneak Peek



Alexander Norell
Global Security Architect

Sept. 17, 2026

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

Welcome.

Involved with PCI since 2006.

Worked both sides of the table.

IT 32 years. Security 26 years.



SPEAKER

Alexander Norell

Global Security Architect, VikingCloud

QSA, P2PE Assessor, P2PE Application Assessor, SSA, SSLCA, QPA, 3DS Assessor, CISSP, CSSLP, CCSP, AAISM, CISM, CISA, CRISC, CDPSE, CCOA

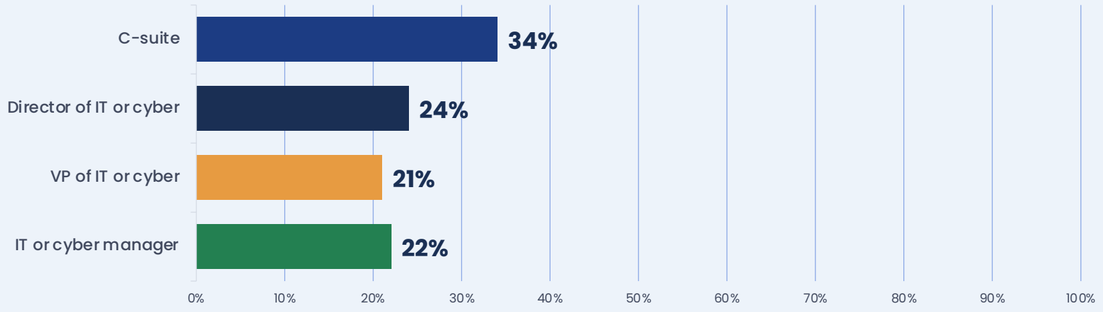
VIKINGCLOUD®

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

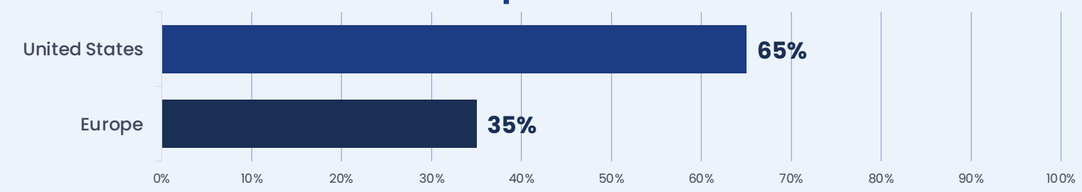
Key survey demographics:

We surveyed 200 security and IT decision makers at large, multi-location brands—in the U.S. and Europe.

Role

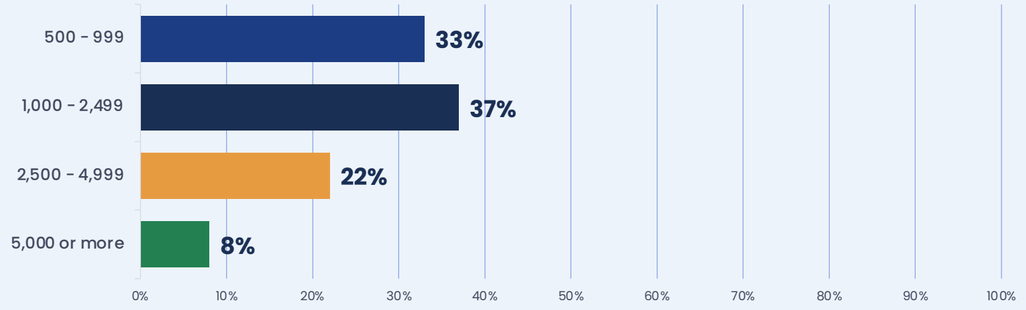


Headquarters

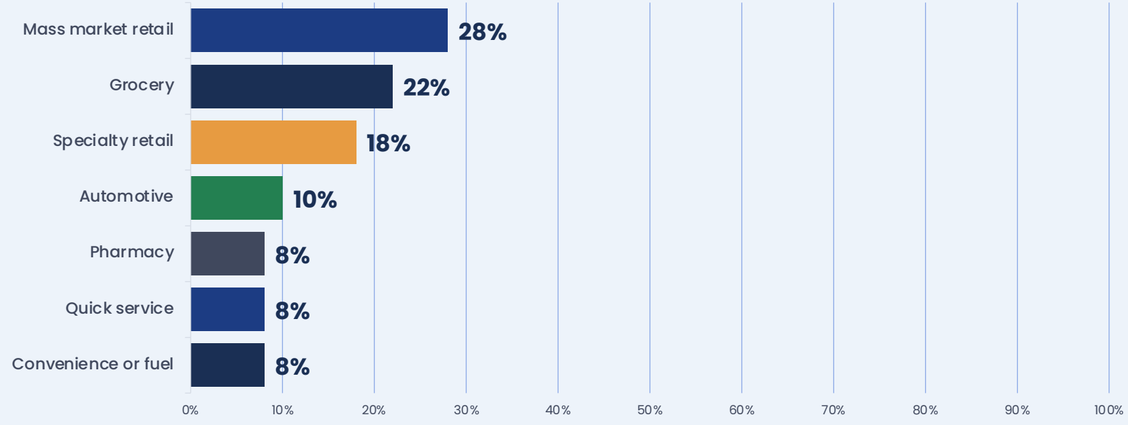


Europe: United Kingdom 10%, Ireland 10%, Germany 8%, and France 8%.

Locations operated



Sector



VIKINGCLOUD®

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

What they told us.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

They feel protected.

Their confidence tracks what they have built: policy, staffing, and technology.

83%

are confident or very confident in their organization's cybersecurity posture.

Policy

98%

have a formal cybersecurity policy across their locations, a security team, and enterprise-grade defenses.

Technology

6

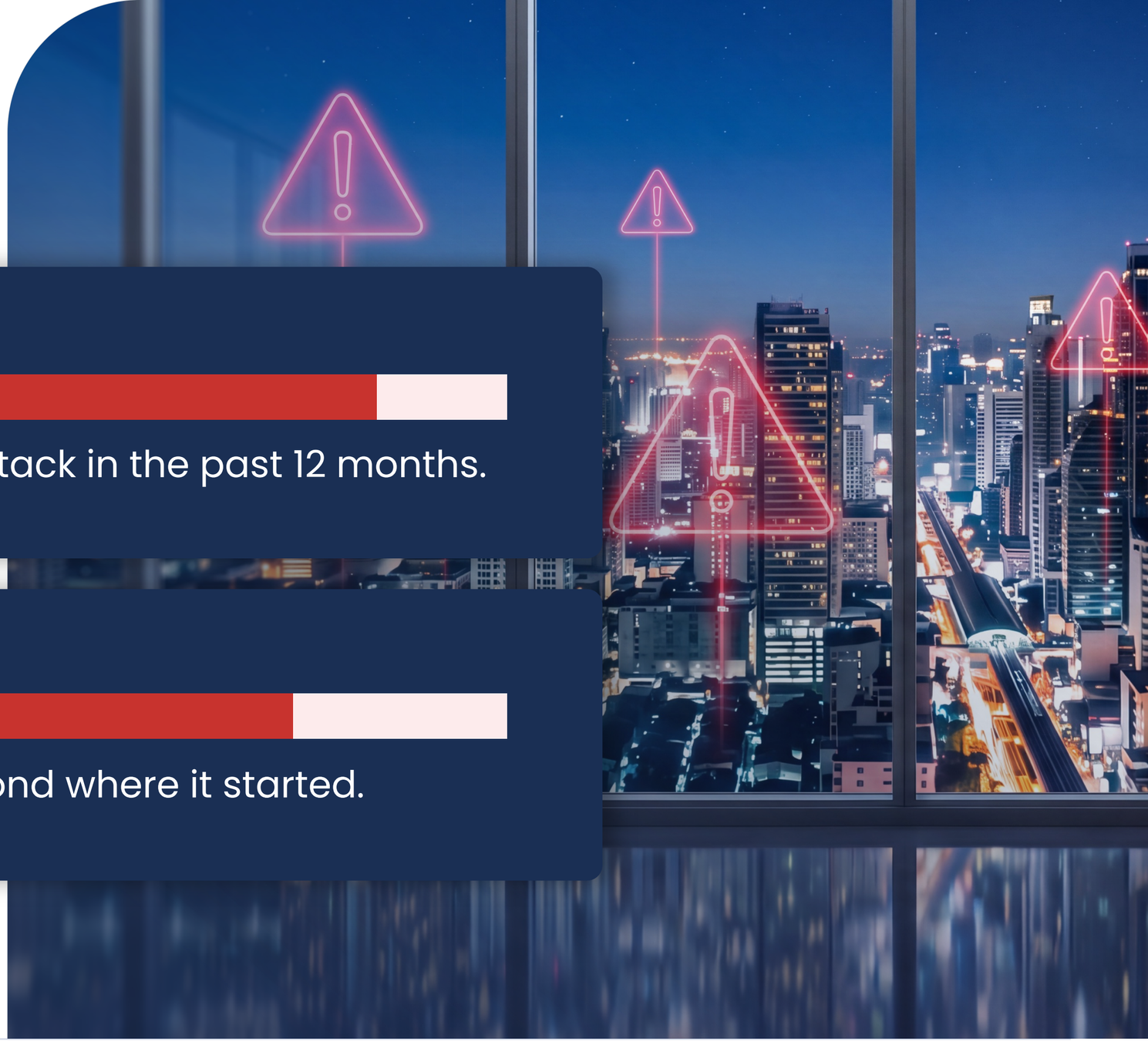
of the 13 security technologies measured are deployed on average.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

How do we know their confidence is just an illusion?

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

Most multi-location enterprises have been attacked.



86%

experienced a cyberattack in the past 12 months.

77%

of attacks spread beyond where it started.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

Bigger is not safer.

More locations mean more routes in, and more places for an attack to travel.

Blast radius by footprint size.

How far an attack travels beyond where it started:

89%

2,500 or more

locations.

71%

500 to 999

locations.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

The Distributed Enterprise Illusion:

The belief that a **strong security plan set at the center by a well-defended headquarters** means consistent protection at every location a brand operates.

It doesn’t.



VIKINGCLOUD®

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

For half of distributed enterprises, cybersecurity policy stops at headquarters.

⚠ 49% **operate with fragmentation of some kind.**

How security policy is set:



51% Corporate mandates one standard.



49% Locations have implementation discretion or set their own policy.

Even among corporate-owned operators,

41%

still do not mandate security policy across all locations.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

Fragmentation has a start date.



80%

of distributed enterprises **do not fully integrate** a new location into central cybersecurity monitoring and enforcement before or on the day it opens!

Openings are announced in advance. Protection is not.

Every new site is an **open invitation to attackers**, putting all locations at risk.

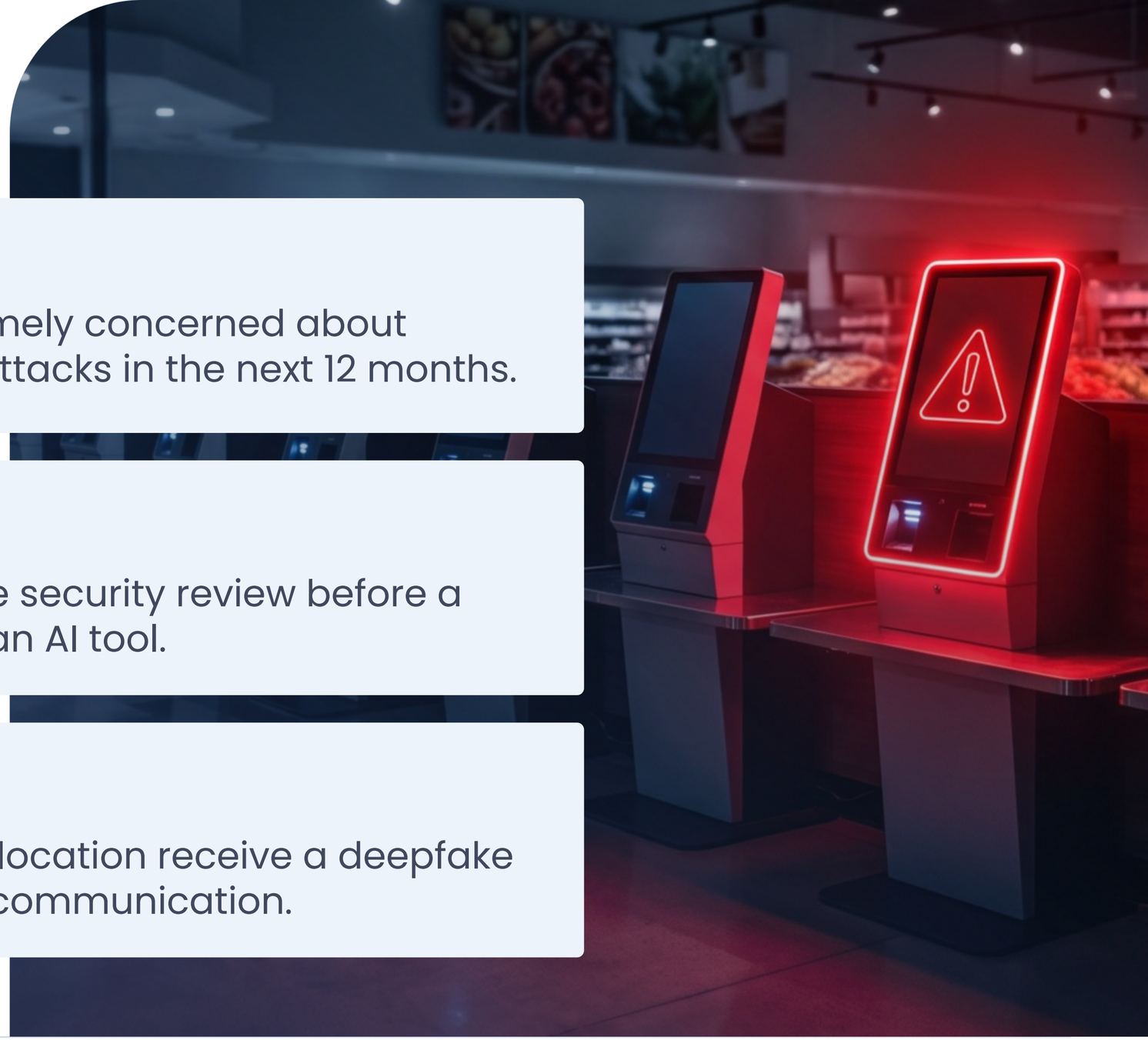
COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

AI is creating more complexity.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

Three new entry points.

All already here. None planned for.



1 Frontier models.

60% are very or extremely concerned about AI-accelerated attacks in the next 12 months.

2 Shadow AI.

Only 4% require corporate security review before a location adopts an AI tool.

3 Location deepfakes.

63% had at least one location receive a deepfake or cloned-voice communication.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

Shadow AI risk is real and growing.

Organizations can't protect themselves when they don't know what AI tools are running across their locations.

Only

4%

of organizations require **corporate security review** before a location adopts an AI tool.

Location-level AI adoption	
Customer service chatbots	**45%**
Employee scheduling	**39%**
Marketing content tools	**38%**
Generative AI tools	**33%**
Point-of-sale systems	**32%**
Inventory forecasting	**26%**
Vendor-embedded AI	**26%**



COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

Leadership’s confidence is being formed on incomplete information.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

They cannot see every site.

And the least-monitored sites are where they expect to miss a threat.

Visibility improves with scale.

Have real-time visibility across all locations, by footprint size.

52% **All** respondents.

44% **500–999** locations.

65% **2,500+** locations.



40%

reported they would likely miss an active threat at their least-monitored sites.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

Leadership does not hear about every important cyber attack.

Missing a threat is one problem. Not hearing about the ones that do get caught is another.

91%

had at least one material cybersecurity incident go unreported to leadership.

79% say multiple incidents went unreported.

43% reported 5 or more.

Underreporting gets worse as the footprint grows.

33% of enterprises with 500–999 locations say five or more incidents went unreported, compared to:

37% of those with 1,000 to 2,499 locations and,

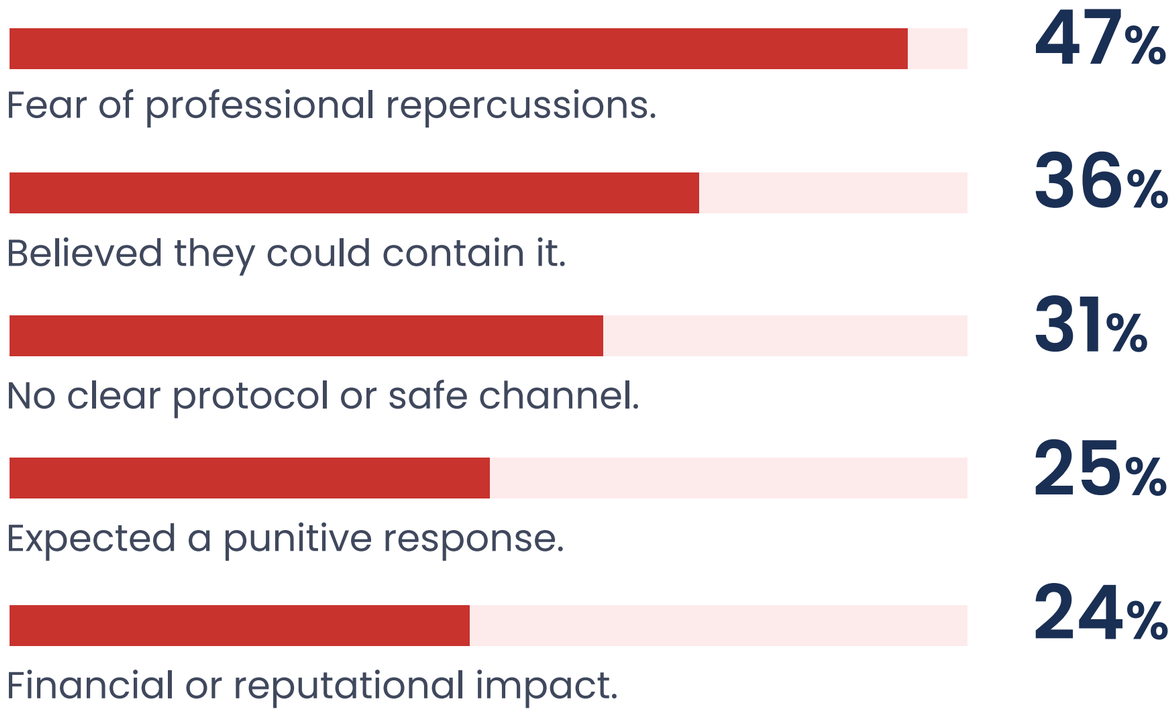
58% of those with 2,500 or more.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

Fear, not confusion.

Why material incidents don’t get reported.

Why incidents went unreported



3rd consecutive year our research has found fear driving the silence.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL



The blast radius has a price.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

A breach across most locations runs to eight figures.

And the damage respondents expect most is commercial, not financial.

47%

estimate a breach affecting a majority of their locations would cost **$11 million or more.**

22%

put it at **$101 million or higher.**

Effects beyond the immediate financial hit.

Loss of consumer confidence	**40%**
Workforce reductions	**36%**
Location closures	**36%**
Higher cyber insurance premiums or exclusions	**33%**
Leadership or executive departures	**28%**
Stock price decline	**25%**

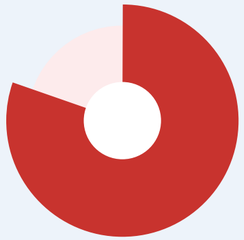
Legal exposure ranks lowest: lawsuits 19%, required disclosure 19%, regulatory fines 18%.



COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

Headquarters owns the bill more often than it owns the control.

Who pays versus who governs.



78% Corporate makes the ransom call.



51% Corporate mandates security policy.

The responsibility gap leaves headquarters **carrying the cost** of incidents in parts of its own network **where it does not set the rules.**

VIKINGCLOUD®

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

What security leaders plan to do next.

VIKINGCLOUD®

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

They are buying more technology.

Respondents plan to nearly double the security technologies they have in place—and to improve their visibility of distributed locations.

The most common additions.

46%

Next-generation firewall centrally managed across all locations.

46%

24x7 managed detection and response (MDR) for every location.

45%

A single platform for visibility across all cyber threats, from an MSSP.

43%

Third-party vendor risk monitoring, including vendors chosen locally.

43%

Endpoint detection and response (EDR) on every device at every location.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

But technology buys confidence. Not containment.

Confidence rises with every technology added. Lateral blast radius does not change.

Will more technology and visibility stop the spread? **No.**

Confidence climbs with the stack:

4 or fewer technologies.	**73%**
5 to 9 technologies.	**87%**
10 or more technologies.	**100%**

% of leaders describing themselves as confident or very confident.

Containment does not change:

Neither real-time visibility nor any of the 13 security technologies measured is associated with less lateral movement.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

What does reduce the blast radius?

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

One mandated standard narrows the blast radius.

For brands with franchised locations, one corporate security mandate makes an attack

3x more likely to stay where it started.

Breaking the illusion:

One brand, one standard.
Mandates make technology work.

Attacks that spread beyond where they started.



64% Corporate mandates one standard.



89% No unified standard.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

How can we break the Distributed Enterprise Illusion?

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

You cannot stop every attack.

But you can narrow the openings, limit the damage, and contain the blast radius.

It starts with 5 steps:

1 Set one standard and make it mandatory.	Deploy the same security stack at every site, from the flagship location to the newest franchise, and extend it to AI.
2 Do not wait for visibility to set the standard.	Waiting for full visibility is the most common reason a standard never gets set. Build visibility, but do not lead with it.
3 Cover a new location before it opens, not after.	Name an owner for day-one protection and make it a condition of opening.
4 Make escalation safe.	Fear of professional repercussions is the top reason incidents go unreported. Create a channel to raise them without immediate blame.
5 Know when to seek expert guidance.	33% already outsource or co-manage security operations. Another 38% plan a partner covering all locations within 12 months.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

Govern, do not just monitor.

> You cannot monitor your w
> out of blast radius.
> **You have to govern.**



Kevin Pierce
President and Chief Operating Officer, VikingCloud

The question is no longer if an attack will happen. It's how far it travels when it does.

The brands best positioned treat **every location as part of a single security program,** whether they own it or not, and make that standard *mandatory.*

VIKINGCLOUD®

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

VIKINGCLOUD®
BUSINESS UNINTERRUPTED.

Thank you.
Questions

Alexander Norell
Global Security Architect

Sept. 17, 2026

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL

VIKINGCLOUD®
BUSINESS UNINTERRUPTED.

Confidentiality and Proprietary Information Notice

All information contained herein is the confidential and proprietary information of VikingCloud.

These materials are provided for informational purposes only and do not constitute a representation or warranty by VikingCloud. The information contained herein may not be reproduced, published or distributed to any third parties without the express prior written consent of VikingCloud.

VikingCloud and the VikingCloud logo are trademarks of VikingCloud, Inc. and/or its affiliates in the United States and other countries.

COPYRIGHT © 2026 VIKINGCLOUD, INC. OR ITS AFFILIATES. CONFIDENTIAL