Achieving Cybersecurity Success in Canada

Research insights from 400 Canadian CISOs

Bell

Contents

Introduction and key findings

As cloud, GenAI, and other technology advances accelerate the capabilities of business – and of threat actors – security leaders face difficult decisions.

There are many choices to make when evaluating the increasing variety of products, services, frameworks, and standards that all claim to be vital to a successful security program.

We surveyed 402 Canadian organizations across the public and private sectors to learn how they are achieving key outcomes, and to see what activities might spur improvements. Discussed in further detail on the next page, those outcomes include:

- Meeting/exceeding compliance objectives;
- Having high confidence in their security posture;
- Achieving the best possible rates for cyber insurance;
- Having highly satisfied security staff;
- Not experiencing a cybersecurity breach in the past 12 months.

The survey asked about a range of factors spanning organizational culture, governance, business alignment, and cloud security practices. By identifying factors/activities that correlate with these outcomes, our goal is to provide security leaders with an informed perspective as they evolve strategies for protecting their organization, with a particular focus on securing the cloud.

Overall, the top success factors for cloud security are 1) the integration of security and DevOps, 2) establishing an acceptable-use policy for cloud services, and 3) how responsive that security teams are to business and IT needs. We dig into those factors, and many more, in the pages that follow. Below are highlights of the lessons learned from the study that we will go into more detail, further in this report:

Nearly **two-thirds** of Canadian organizations had breaches in the last year. Almost half occurred in cloud environments.

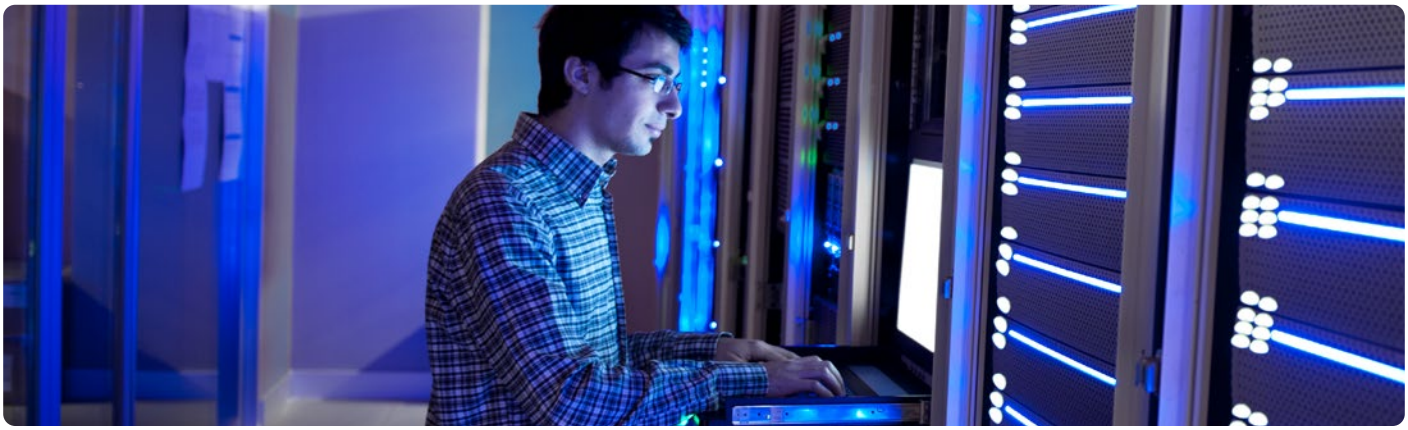
Just **1.6%** of organizations report high achievement across all five of the security outcomes we tested.

29 success factors correlate with significantly higher success rates for at least one outcome. In this report, we identify the clusters that drive the most success.

2 We identify two factors that were the most crucial for reducing the likelihood of breaches.

About the survey

Bell Canada hired professional research firm Maru Group, to conduct a stratified random sample of approximately 402 security professionals working for organizations in Canada. Response targets were set to achieve a balance of respondents representing different industries, provinces, and organization sizes. Quality checks eliminated some responses, leaving a final sample of 383 for this analysis. You can find demographics for this sample in the Appendix.



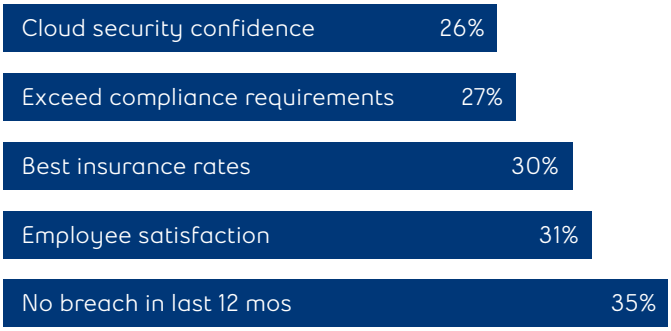
Security program outcomes

What is clear from our latest study is that there were a few common themes: While breaches are the most direct performance indicator of any security program, most CISOs that we surveyed found performance against compliance requirements and the ability to retain talented staff as important indirect indicators.

In developing our survey, we added a company's overall confidence in its cloud security as well as the third-party perspective that comes with a cybersecurity insurance valuation. The survey posed representative questions that assess the organization's level of success for each of these five objectives.

These are not the final word in measuring the success of a security program, but they do serve as a good measurement framework for our analysis. Below is how organizations assessed their ability to attain each of these outcomes. It is worth noting that many organizations reported a high level of achievement across multiple outcomes, but only 1.6% of respondents reported a high level of achievement for all five.

Figure 1: Percentage of respondents reporting strong success, per outcome



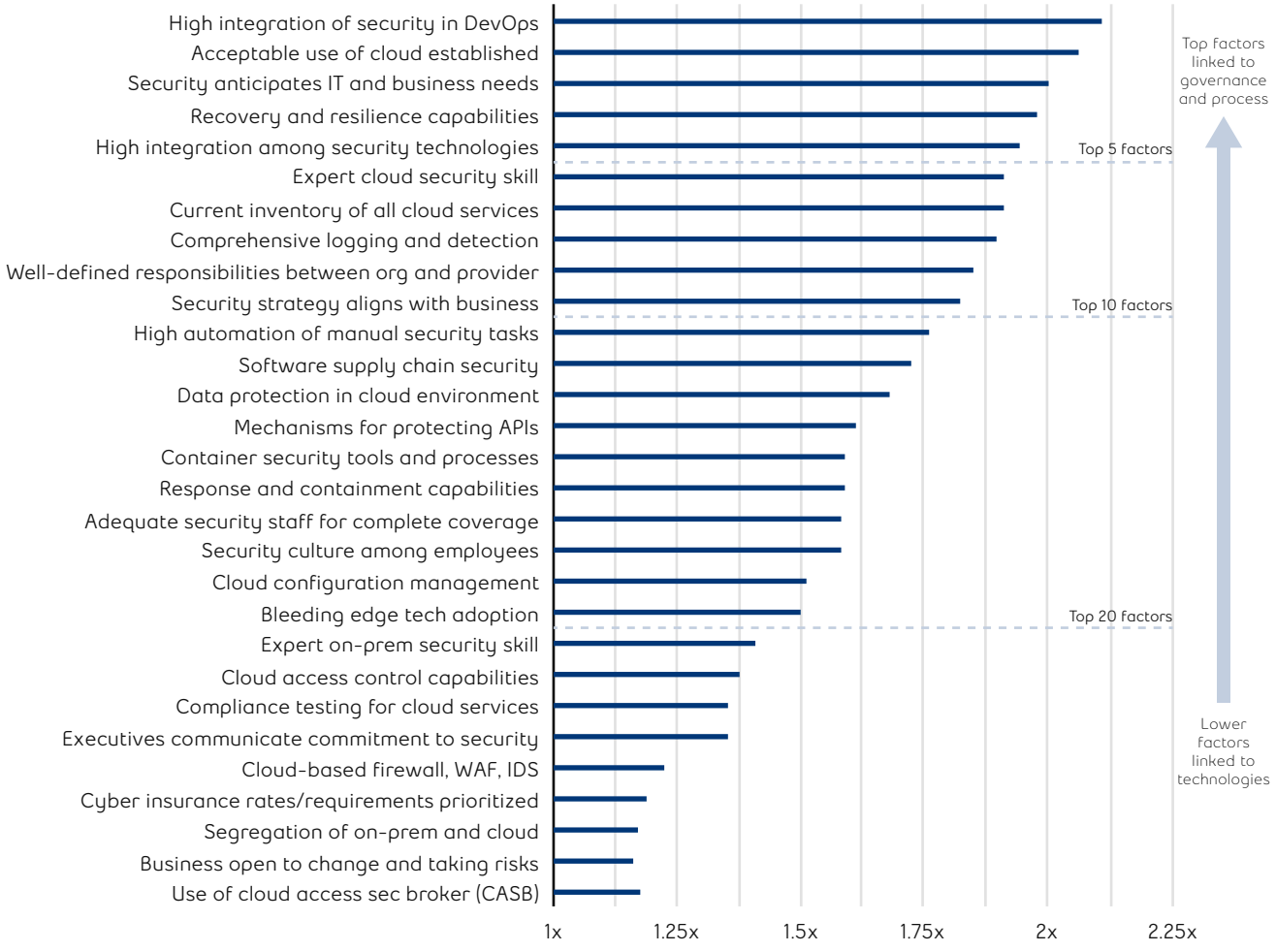
- Cloud security confidence. 26% of respondents express a high degree of confidence in the ability of their security program to adequately protect business activities in the cloud. This being the lowest rate among the five outcomes speaks to the cautious nature of the respondents, in addition to the many challenges of security in cloud environments.
- Regulatory compliance. 27% of organizations report exceeding compliance requirements, and 26% express strong confidence in their cloud security capabilities. Compliance tends to instill confidence, so it is not surprising to see similar opinions on those outcomes.
- Cyber insurance. 30% of respondents say that their firms get the best cyber insurance rates. Since many insurers conduct risk assessments and due diligence to set those rates, this can be seen as a third-party assessment of risk posture. Clearly, organizations will use other means to validate their posture, but an insurer's assessment is a useful perspective.
- Staff satisfaction. About 3 in 10 organizations enjoy very high rates of satisfaction among security employees. Earning higher scores on employee satisfaction has a causal link to the already difficult task of retaining security talent. Success in your position, alongside the ability to innovate and explore newest/latest technologies and practices, all serve to improve employee satisfaction.
- Security breaches. While 35% of respondents reported that their business did not experience a breach during the previous 12 months, it is worth noting that some might have been unaware of a breach. This only serves to emphasize the associated conclusion: at least 65% did experience a breach.

Security program success factors

To identify factors that correlate with our chosen success outcomes, we asked respondents numerous questions about their organization's governance, security staff, and cloud security practices. The resulting data enabled us to not only establish correlation, but also determine how much each factor increases the likelihood of an organization reporting the highest level of achievement for each outcome.

In all, we identified 29 factors that correlate with significantly higher success rates for at least one outcome. We show these in Figure 2, where the numbers along the x-axis represent the average improvement for each factor across the five outcomes. **For example: organizations reporting strong recovery and resilience capabilities (the 4th highest factor) report success rates that double (2x) those with lower integration**. We categorize and highlight these factors in the sections that follow.

Figure 2: Factors showing significant positive correlation with at least one security outcome.



Organizational culture

In our previous survey, we learned that over-reliance on technology (to the detriment of people and training) can lead to suboptimal outcomes. Moreover, inadequate governance and/or security culture can undermine even the best talent and tools that money can buy. Therefore, before examining technical controls, we start with governance and culture.

Figure 3 lists the governance and culture factors that we surveyed in conjunction with the five outcomes of our analysis framework. The values in each cell represent the average increase in an outcome's success rate that correlates to that factor. **For example: organizations that do the best at establishing and enforcing governance for the acceptable use of cloud services are twice as likely to report exceeding compliance requirements.** Blank table cells indicate no significant impact between the factor and outcome.

Figure 3: Increase in successful outcomes associated with governance and culture factors

		Security outcomes				
		Exceed compliance requirements	High confidence in security	Low insurance rates	Satisfied security staff	No breach
Program input factors	Acceptable use of cloud established	2x	2.4x	2.3x	2.6x	
	Well-defined responsibilities between org and provider	2x	2.1x	2.1x	2.1x	
	Security strategy aligns with business	2.1x	2.1x	2x	2x	
	Bleeding edge tech adoption	2.2x	2.1x		2.1x	
	Security culture among employees		1.9x	2x	2.1x	
	Executives communicate commitment to security			1.9x	2x	
	Cyber insurance rates/requirements prioritized			2x		
	Business open to change and taking risks					1.9x

Why are breaches an outlier?

It might seem counterintuitive: the only governance factor that coincides with a significantly reduced likelihood of reporting a breach is a mentality among business leaders to embrace change and be open to taking risk. In fact, being open to change (and calculated risk) can mean the early adoption of new technologies, improved employee morale, and other factors.

Establish responsibility and acceptable use

Establishing the level of risk for acceptable use of cloud services is a strong overall factor across the outcomes. Key to establishing acceptable risk levels is a clear delineation of who is responsible for each aspect of managing risk. This relates to the internal responsibility of business, IT, security, and other stakeholders. It also relates to the shared responsibility of cloud security that hyperscalers have been promoting for some time. Defining risk and responsibilities starts with good governance that is then implemented across many security controls, including cloud configuration management and access controls.

Align with business

It is not surprising – organizations reporting close alignment between their business and security strategies were more likely to achieve stronger outcomes across the board. This lends credibility to the recently created role of the Business Information Security Officer (BISO) now in place at some large organizations.

Furthermore, a strong executive commitment in support of the security initiatives needed to implement that strategy is linked to higher rates of employee satisfaction – and also to getting the best insurance rates (perhaps because that commitment is evident to insurers).

Be open to experiment

Organizations that say they experiment with and adopt new technologies before most others find it easier to keep both compliance auditors and security staff happy. This also ties in with higher levels of confidence that the security program can adequately protect business services running in the cloud. A culture that encourages experimentation / trying new things can take advantage of new cloud-native approaches to platform and application architecture that are arguably more secure than traditional approaches (e.g., automated checks in advance of production and greater visibility / logging capability from production workloads).

Foster security culture

According to the data, a strong security culture helps drive business confidence in cloud security capabilities, employee satisfaction, and lower insurance rates.

Those first two make complete sense because the surrounding environment fosters confidence and satisfaction (as are doubt and dissatisfaction). The correlation between culture and insurance rates might seem odd, but a pervasive culture of security will likely have a positive influence on an insurer's assessment.

Bell's recommendations

Track metrics that matter

Good governance needs support from a foundation of healthy metrics. The most impactful set of metrics tend to cover the widest breadth of assets. Building metrics around your inventory of assets and exposures is a natural starting point. Questions to answer include:

- How much attack surface coverage do I have?
- What is the change in exposure?
- How much time does it take to resolve issues?
- How quickly can we reduce our backlog of issues?

Fail fast

Create a culture that is comfortable learning and trying new things. Sometimes you need to take a leap of faith and try something where solid metrics are not yet available. Taking full advantage of the cloud – including the flexible architecture, rapid development and increased security automation – means being open to experimentation within defined guardrails.

In a cloud-native world, governance is more easily reflected in software such as Policy as Code to manage risk in real time and/or limit the downside of experimentation. Organizations that achieve better security outcomes indicate that they embrace change. For example, organizations using Large Language Models (LLMs) such as ChatGPT for security operations in production show improved security outcomes.

Success factors for security teams

Figure 4 has 20 factor-outcome intersections, five of which show at least 2.5x improvement. Compare that to only one (of 40) in Figure 2. People are powerful drivers of positive outcomes.

Figure 4: Increase in successful outcomes associated with teams and talent

		Security outcomes				
		Exceed compliance requirements	High confidence in security	Low insurance rates	Satisfied security staff	No breach
Program input factors	Expert cloud security skill	2x	2.6x	2.6x	2.5x	
	Security anticipates IT and business needs	2.1x	2.5x	2.2x	2.2x	
	Adequate security staff for complete coverage		2.6x		2.3x	
	Expert on-prem security skill	2x			2.1x	

Make new friends

In the last section, we saw that organizations reporting a more open approach to technology adoption also report it easier to achieve our measured outcomes. Naturally, this goes hand in hand with strong collaboration with IT and other stakeholders. The results in Figure 4 corroborate this more collaborative approach. Security teams able to anticipate and respond to the needs of the business and IT organization see improvement in four of five outcomes.

Collaboration between security and other teams becomes more important in the cloud – where IT and security visibility may not be straightforward. For example, cloud configuration management, identity management, and data security are each areas where security personnel may not have complete control, needing to rely on the ready participation of others in IT and across the business.

Grow numbers and knowledge

Many organizations share that they are short-handed when it comes to their security staff. From budget constraints to difficulty filling open jobs, it is easy to feel overwhelmed when understaffed. Not surprisingly, we see gains in confidence and satisfaction among security programs that have adequate staffing to cover operations.

Nevertheless, the data attributes even more benefits to security teams that are highly skilled at what they do. Strong cloud security skills appear especially effective at improving outcomes. Skill specializations are important and add to comprehensive capabilities to protect an organization wherever it operates.

Bell's recommendations

Go beyond certifications

The skills that security teams seek are expanding across more domains (e.g., cloud-native controls) as well as deepening (e.g., more coding). Traditional technical skills and certifications remain important, but this research shows that business knowledge, AI capabilities, and coding each factor prominently in the must-have skill sets of security professionals. Staff training and recruitment in these areas are much more important for cloud security than in traditional on-premises roles.

Extend the definition of team

To improve security staff retention, work to reduce the friction that they experience in asking others to take action (e.g., fixing misconfigurations, accepting downtime for updates, addressing coding issues, minimizing access permissions, etc.). This requires agreement across business stakeholders, developers, IT, and security on what an acceptable level of security risk is – which links back to our section on Governance and Culture.

Cloud security practices

In this section, we unpack the technical and procedural controls that measurably improve security outcomes. Having asked respondents to rate the implementation of various cloud security practices at their organizations, we then correlated those answers against the five outcomes. Figure 5 lists the top practices in terms of overall improvement across all outcomes.

Figure 5: Increase in successful outcomes associated with cloud security practices

		Security outcomes				
		Exceed compliance requirements	High confidence in security	Low insurance rates	Satisfied security staff	No breach
Program input factors	Current inventory of all cloud services	2x	2.6x	2.5x	2.5x	
	Recovery and resilience capabilities	2x	2.2x	2.1x	2.6x	
	Comprehensive logging and detection	1.9x	2.2x	2.2x	2.2x	
	Software supply chain security	2x	1.9x	1.9x	1.8x	
	Data protection in cloud environment		2x	2.3x	2.2x	
	Mechanisms for protecting APIs		2.1x	1.8x	2.1x	
	Container security tools and processes		2.2x	1.8x	2x	
	Response and containment capabilities		1.9x	2x	2.1x	
	Cloud configuration management		1.9x	1.8x	1.9x	
	Cloud access control capabilities		2x		1.9x	
	Compliance testing for cloud services		1.9x	2x		
	Cloud-based firewall, WAF, IDS					2.2x
	Segregation of on-prem and cloud	1.9x				
	Use of cloud access sec broker (CASB)		1.8x			

The above list of promising practices for improving cloud security is quite varied. Below, we highlight several themes across multiple practices.

Know what you're protecting

There is a reason why the NIST Cybersecurity Framework (and many other security frameworks) start with the 'Identify' function of a security program. It is hard to defend something if you don't know where it is, how it's configured – or that you have it at all. This is especially important in the cloud, where resources are distributed and ephemeral by nature.

This supports our findings that organizations with an up-to-date inventory of all cloud services saw the highest overall gains to security outcomes. Having knowledge of what is running or stored in the cloud today is key to convincing auditors, insurers, or even your own staff that you can adequately protect it tomorrow. All security controls depend on this basic, yet difficult-to-achieve starting point of simply knowing which services are being used and what they connect to. In this way, inventory management, risk management, configuration management, software supply-chain management, and attack-surface management are closely tied together – and underpin a successful overall cloud security strategy.

Plan for success; build for failure

The NIST Cybersecurity Framework ends with 'Respond' and 'Recover.' Naturally, executing a strong response and rapid recovery relies heavily on an up-to-date inventory of cloud services, including their configurations, users, and data. Recovery and resilience capabilities rank #2 overall for driving outcomes, while ensuring that swift response and containment ranks in the middle of the pack.

Responding to and recovering from failures requires mechanisms in place to know when those failures occur. Accordingly, comprehensive logging and detection feature prominently in Figure 5. While our survey did not focus on what should be logged and which detection mechanisms work best, this analysis does offer strong justification for asking

those questions within an organization.

Develop cloud-native protection controls

Architecture and administration are done differently in cloud environments. Accordingly, cloud protections have evolved to fit them. We see evidence of this in Figure 5, where no fewer than nine practices fall under the banner of cloud-native protection.

These practices range from porting traditional on-premises controls to the cloud (e.g., firewalls), controls that are relevant to cloud infrastructure (e.g., securing APIs and containers), and preventing the ability of adversaries to pivot from compromised on-premises infrastructure into cloud environments (e.g., securing Active Directory).

We also see a reminder that cloud security policies need to be enforced (e.g., via CASB, policy-as-code, etc.) and configurations continuously monitored/managed through the implementation of technical guardrails. Furthermore, organizations that develop their own cloud applications are encouraged to gain visibility into their software supply chain to ensure that vulnerable third-party libraries do not undermine their cybersecurity efforts.

Leverage integration and automation

When analyzing the data on practices that correlate with security outcomes, the theme of integration and automation stand out as particularly strong. We have pulled this data out in Figure 5 to highlight it below. Compared with its predecessor, Figure 6 is noticeably more impressive, including the strongest factor-outcome effect in the entire dataset: high automation of security tasks correlates strongly with getting the best insurance rates (and the attendant external validation of processes and controls).

Figure 6: Increase in successful outcomes associated with integration and automation

		Security outcomes				
		Exceed compliance requirements	High confidence in security	Low insurance rates	Satisfied security staff	No breach
Program input factors	High integration of security in DevOps	2.1x	2.6x	2.3x	2.6x	
	High integration among security technologies	2.3x	2.5x	1.8x	2.2x	
	High automation of manual security tasks		1.9x	2.7x	2.2x	

Automating security controls such as attack-surface management, initial detection, elements of response playbooks, and access control management are highly important for scaling security operations.

Bell's recommendations

Automate as much as possible

This does not come without its challenges: critical cloud security controls such as configuration management may be challenging to fully automate. It may be technically simple to catch and fix misconfigurations, but ensuring that security actions do not inadvertently cause availability issues for business stakeholders is also at issue. We recommend assuming the 80/20 rule, where the majority of fixes should be automatic, but 20% will need some sort of manual/personal intervention).

Adopt platforms instead of point products

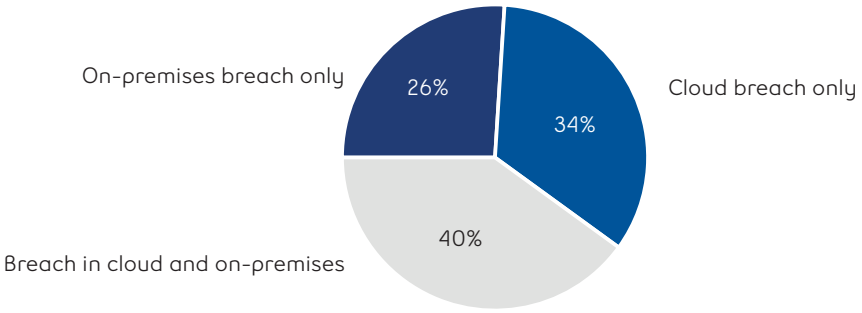
With the rapid evolution of cloud capabilities, keeping the number of tools in check is a challenge, but it will positively affect security outcomes. Furthermore, trying to retroactively integrate disparate technologies is often also difficult (and frequently results in poorer outcomes). The security industry is seeing a faster pace of consolidation into CNAPP and SASE, which will help ease the integration challenges.

Security breaches

From the results we have shared, the majority of organizations reported breaches, and yet very few of the factors that we tested correlated with a decrease in the likelihood of a breach. Because so few factors correlate with a measurable reduction in breaches, we've opted to do a deeper dive into this outcome – and to offer some hypotheses as to why that might be the case.

We begin by unpacking the breach outcome a bit more. Out of our 383 respondents, 249 reported a breach in the past 12 months. For organizations reporting a breach, the most common response was that these events occurred in both cloud and on-premises environments (40%). Among the rest, breaches in cloud infrastructure (34%) were more common than those on-premises (26%).

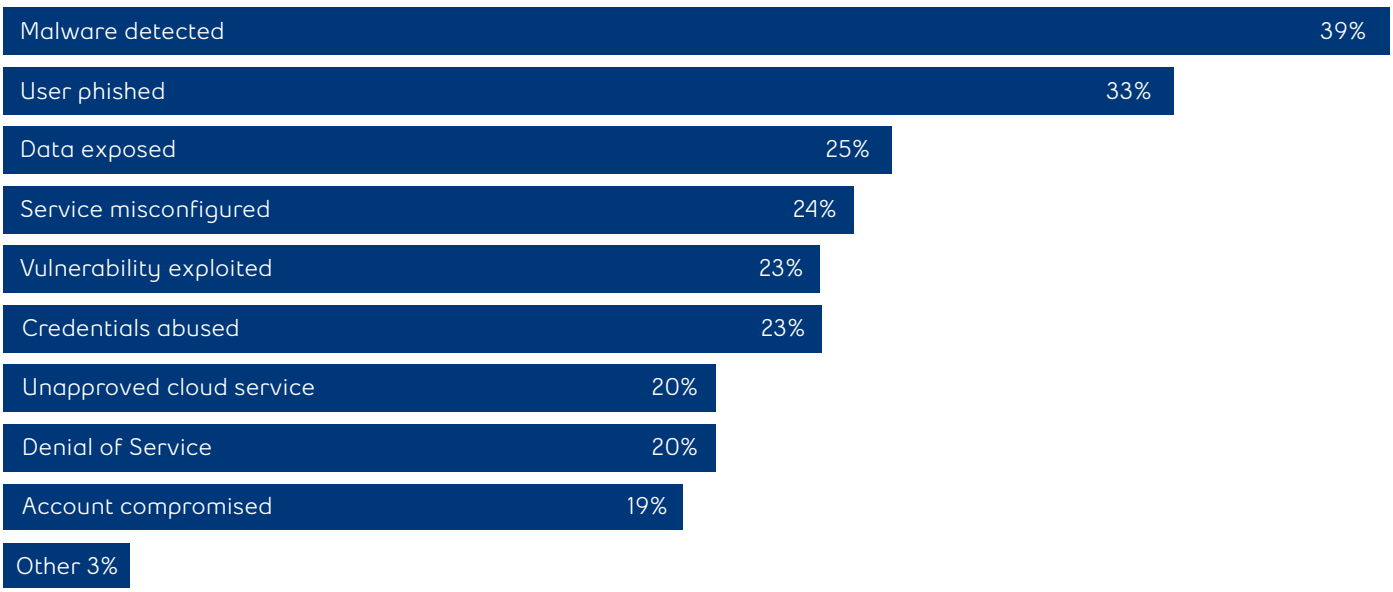
Figure 7: Proportion of organizations reporting breaches in cloud and on-premises environments



Top incidents

We asked respondents about the threat methods and vectors experienced in the previous twelve months, regardless of whether they resulted in loss. Not surprisingly, malware and phishing lead the rest in Figure 8, each contributing to one-third or more of reported incidents. However, the others aren't far behind, reminding us that security incidents rarely have a single cause or step.

Figure 8: Threat methods and vectors associated with security incidents



While this adds some interesting insight, this chart does not address why very few factors correlate with fewer breaches. We have three hypotheses for this:

Hypothesis #1: Single factors rarely reduce chances of a breach.

Most breaches result from multiple threat actions carried out by adversaries who are often very adaptive. Accordingly, it follows that few individual controls have the power to prevent breaches on their own. In addition, we base our analysis on evaluating the effect of each factor individually rather than in clusters. The results support the understanding that no single activity is particularly effective in isolation.

Hypothesis #2: New practices implemented after a breach.

We asked respondents if their organizations had suffered a breach in the last 12 months, but the survey questions were about their present practices. It is plausible that organizations had a breach a year ago, which motivated them to make major improvements to their security program. That time factor could account for why we are not seeing a correlation between fewer breaches and better practices.

Hypothesis #3: Experiencing a breach does not always include detecting it.

In order to answer "Yes" to our question about the occurrence of a breach, organizations must first have been able to detect that a breach occurred. Further, it is easy to see why so few of the factors we analyze in this report correlate with a lower likelihood of reporting breaches. We should rather expect the opposite. Many security practices should ostensibly improve the organization's ability to detect, and therefore report, breaches. Plus, we do see this positive correlation between factors and reported breaches.

Reflections and recommendations

Organizations with among the highest security budgets are not necessarily the most secure. Other factors identified in this study regarding governance, culture, skills development, employee retention, automation, security practices, and technology selection matter more. While these factors do require financial investment as well as time, it is clear that resource allocation trumps total budget size. Use this study as a guide to help understand how to better allocate your limited resources for improved security success in the cloud and on-premises.

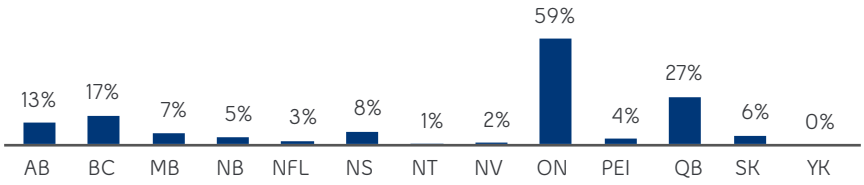
For more information or to talk to a cybersecurity specialist, visit our website.

Bell

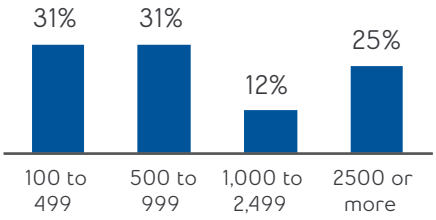
Appendix

Profile of respondents

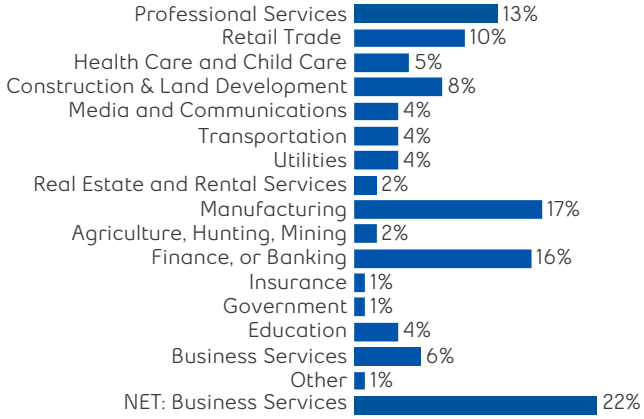
Province of operations



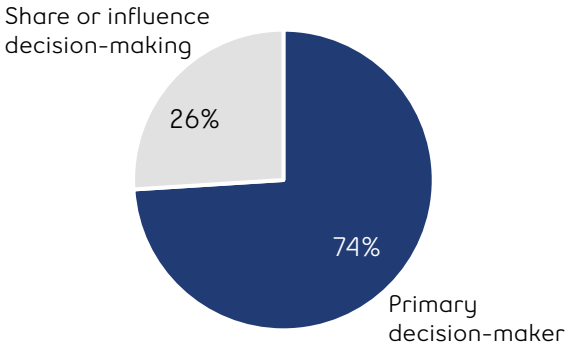
Employee size



Industry



Decision maker



Professional designation