Cybersecurity incidents in SMEs

Research report

Research and Market Intelligence at BDC

September 2024

Table of contents

1 Key highlights

Cybersecurity incidents are a common occurrence nowadays in the business world: most SMEs surveyed have already experienced a cybersecurity incident.

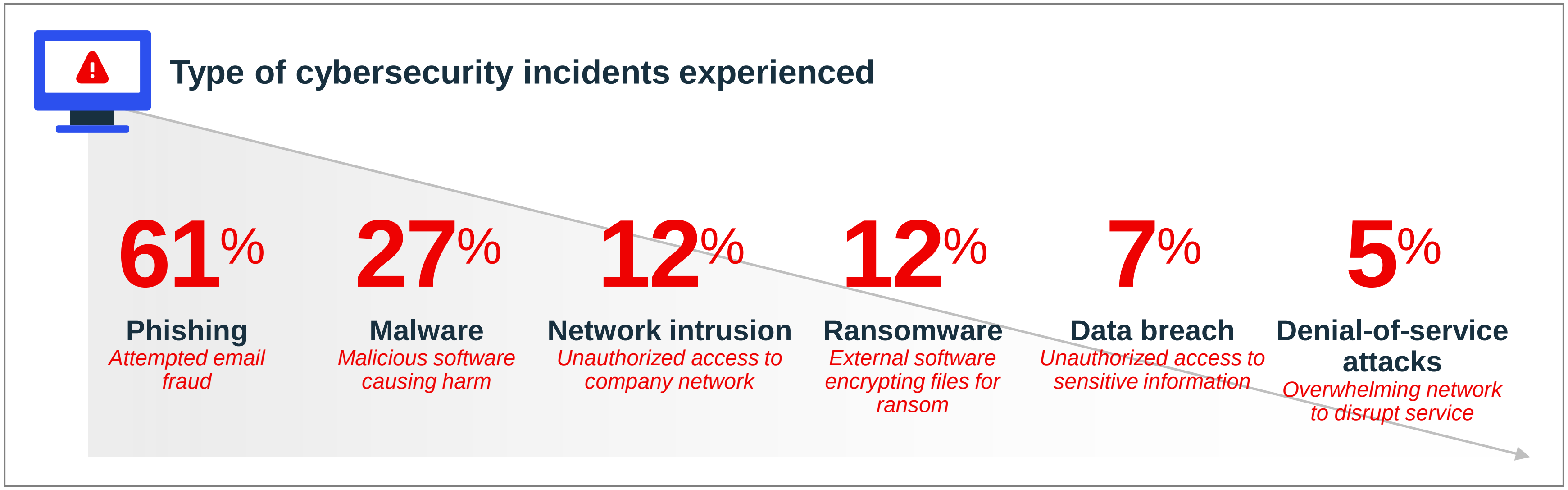
73% Of SMEs **have experienced a cybersecurity incident** in the past

False sense of security?

SMEs with less than $3M in sales are more in agreement with the statement *“The larger the company, the more likely it is to be targeted by a cyberattack”* than larger SMEs.

Still, most small SMEs have already experienced a cybersecurity incident.

Type of cybersecurity incidents experienced



61%
Phishing
Attempted email fraud

27%
Malware
Malicious software causing harm

12%
Network intrusion
Unauthorized access to company network

12%
Ransomware
External software encrypting files for ransom

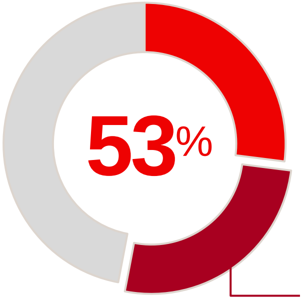
7%
Data breach
Unauthorized access to sensitive information

5%
Denial-of-service attacks
Overwhelming network to disrupt service

Although incidents are quite common these days, a sense of denial seems to persist among Canadian SMEs.

Are you prepared to face an incident?

About half of SMEs do not feel prepared to handle a cybersecurity incident.



Companies that have already experienced an incident are more likely to feel unprepared.

Half of companies that feel unprepared say they are **not at all** prepared to handle them (26%).

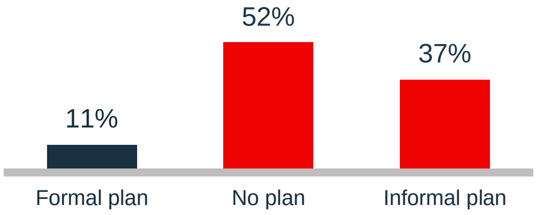
Are you aware of the risks?

20%

Of SMEs **never** assess the risks associated with their partners, suppliers and clients.

Do you have a plan in case of an incident?

Almost all SMEs surveyed have **no** formal response plan in place. Moreover, 30% of those who do, never test it.



A considerable proportion of SMEs were not affected by the incidents they experienced. For some, however, the repercussions have been more serious. The impacts clearly differ from one type of attack to another.

Phishing

Attempted email fraud

Phishing incidents reported by the SMEs surveyed seem to have less impact on the company than other types of incident.

Less than half of respondents said they have cybersecurity trainings in place for their employees. Increasing the proportion of SMEs who train their employees to identify the fraudulent emails could help reduce the number of phishing incidents.

Among those who experienced a phishing incident…

52% said they were impacted by it (vs. 76% for other incidents)

51% said there was no cost associated with the incident (vs. 26% for other incidents)

79% said it took them less than one week to recover from the incident (vs. 66% for other incidents)

Other incidents

Malware, ransomware, network intrusion, data breach and DDoS

While other types of incidents are less common than phishing, their impact on SMEs is considerable.

Among the incidents reported, data breach incidents seem to have the greatest impact on SMEs. Recovery time and costs are at their highest with this type of incident.

Most **common impacts** of those who experienced at least one of these types of cybersecurity incidents:

Disruption of operations (58%)

Increased security costs (35%)

Significant unplanned expenses (31%)

2

Methodology

Methodology

Survey methodology

Online survey.

Respondent profile

Business owners and business decision-makers members of BDC’s ViewPoints online panel.

Survey dates

September 10 through 20, 2024

Margin of error

For a probabilistic sample of 500 respondents, the maximum margin of error is ± 4.4 percentage points, 19 times out of 20. However, as this survey is based on a non-probabilistic sample, this information is provided for reference only.

Data processing and analysis

Were performed by the BDC Research and Market Intelligence team.

Weighting factors

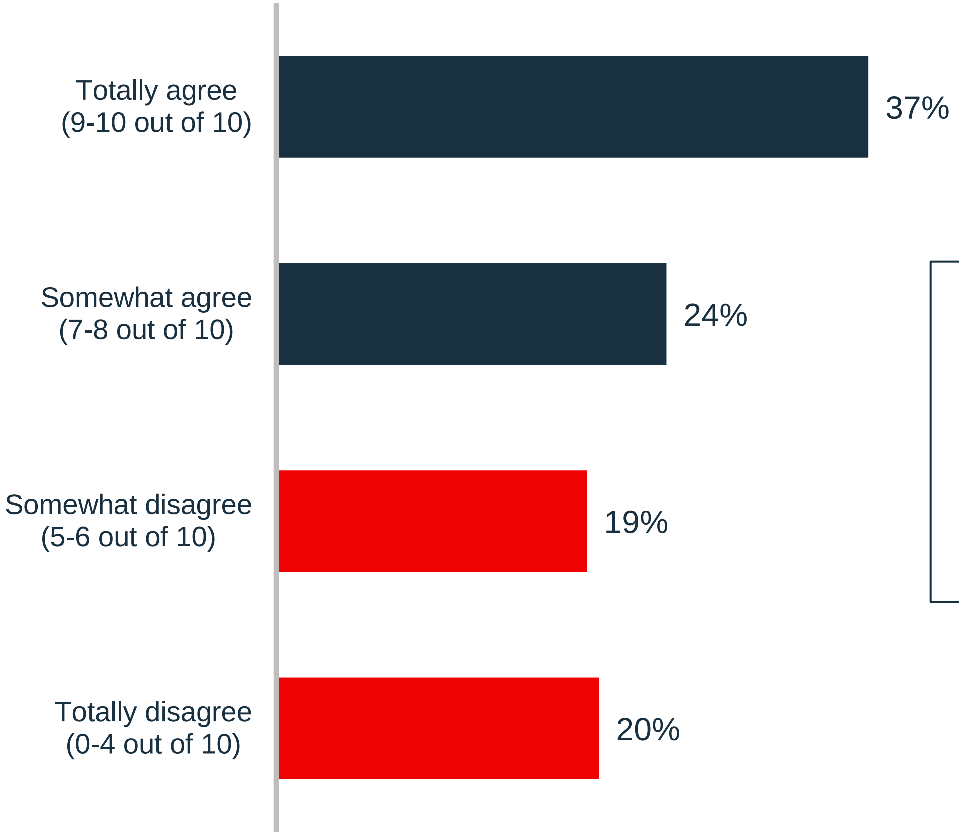
Results were weighted by region and number of employees to be representative of the Canadian SME population.

3 Detailed results

A majority of respondents agreed with this statement. Companies with less than $3M in revenues are more likely to agree with it, and therefore feel - mistakenly - less targeted by cyberattacks.

S3Q1a. To what extent do you **agree** with the following statements?

The larger the company, the more likely it is to be targeted by a cyberattack



Totals

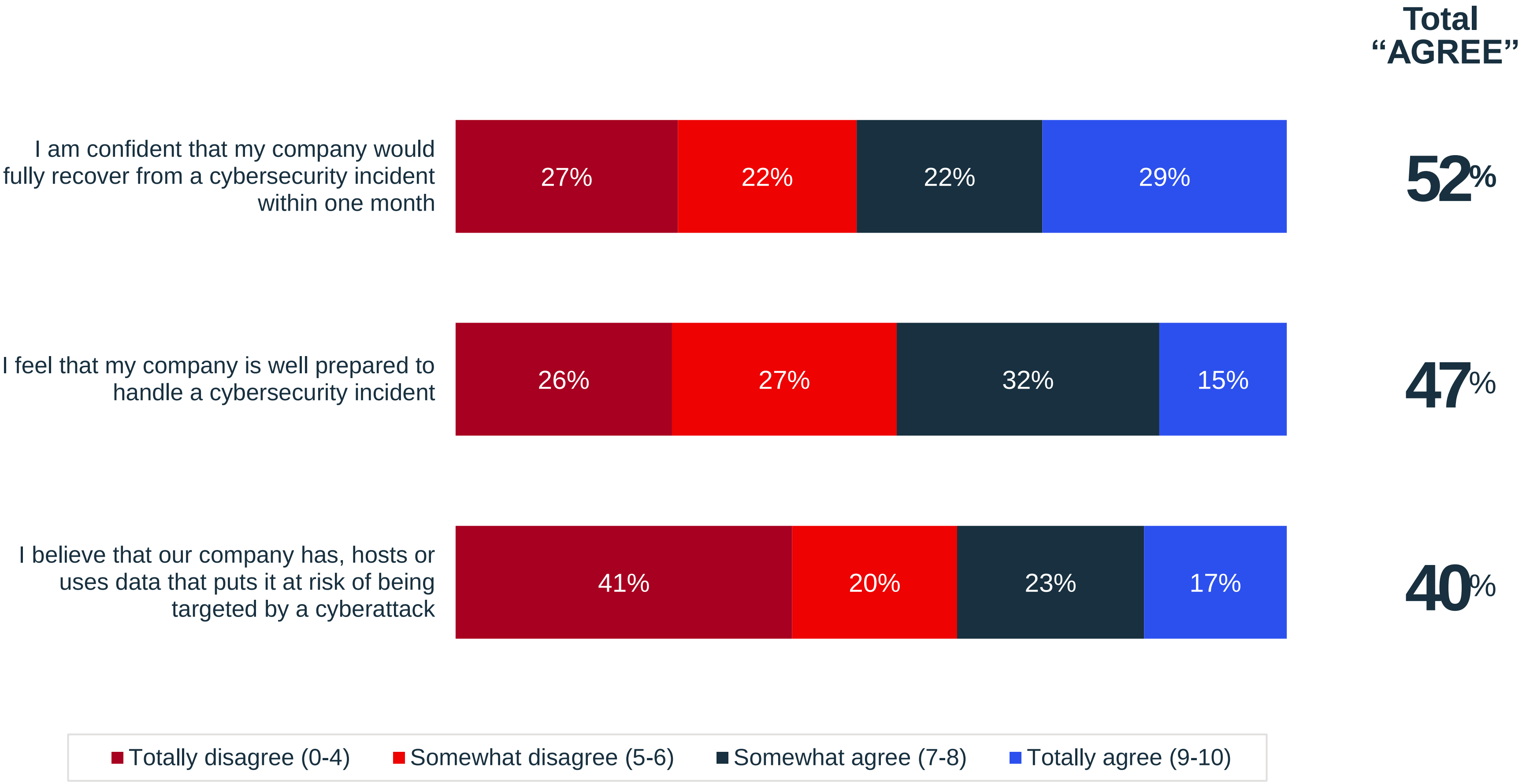
AGREE **61%**

DISAGREE **39%**

Base: All respondents (n=480). Those who did not know were excluded from the calculation base.

Just over half of respondents **do not** feel their company is prepared to handle a cybersecurity incident. SMEs that have already had an incident are significantly less likely to feel well prepared.

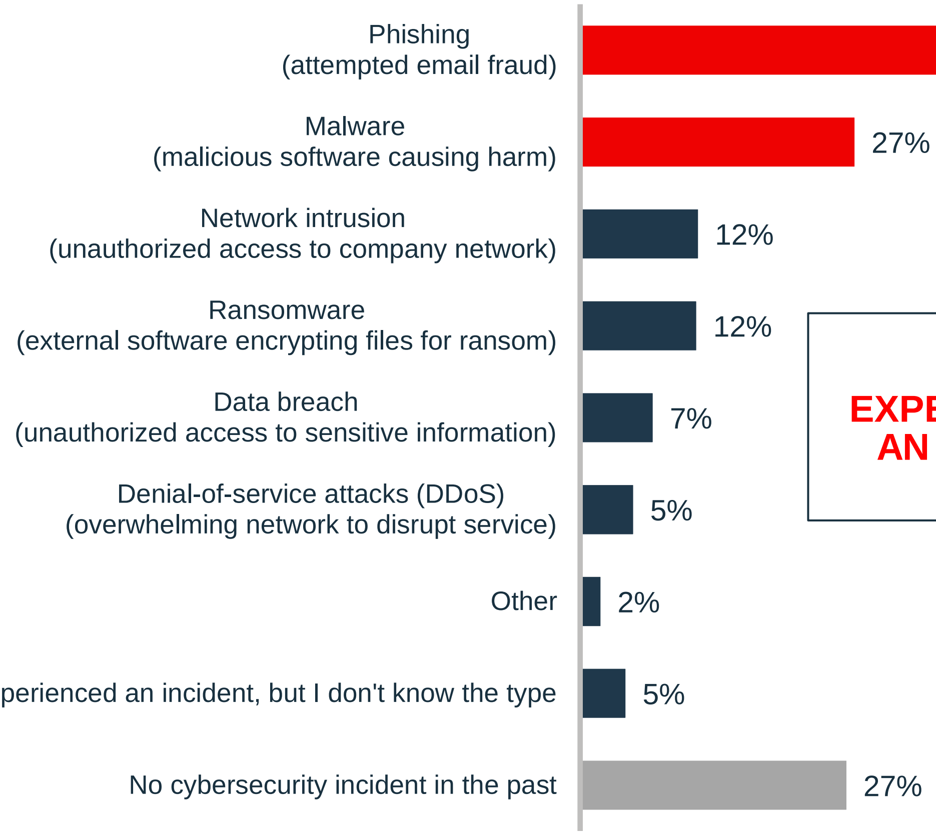
S3Q1. To what extent do you **agree** with the following statements?



Base: All respondents (n=475-487). Those who did not know were excluded from the calculation base.

Most SMEs surveyed have experienced a cybersecurity incident. This is more likely the case among businesses with sales of $10M or more, mainly due to a higher proportion of phishing.

S3Q2. Has your company ever experienced **cybersecurity incidents** in the past?

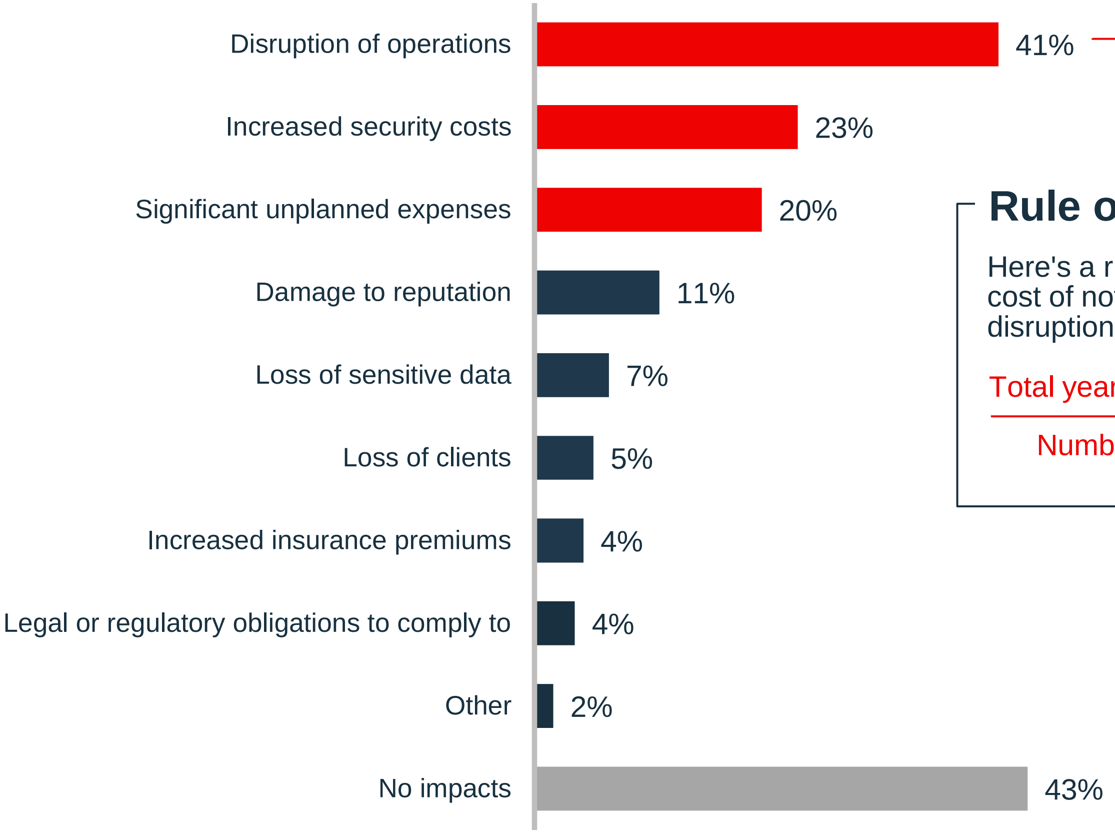


HAVE EXPERIENCED AN INCIDENT 73%

Base: All respondents (n=494). Those who preferred not to answer were excluded from the calculation base. Multiple mentions were allowed, therefore total exceeds 100%.

Cybersecurity incidents mostly impact operations. However, not all incidents have the same degree of impact. Phishing incidents impact SMEs the least, whereas ransomware and DDoS have the largest impact.

S3Q3. What were the **impacts** of the **most recent** cybersecurity incident on your company?



Rule of thumb

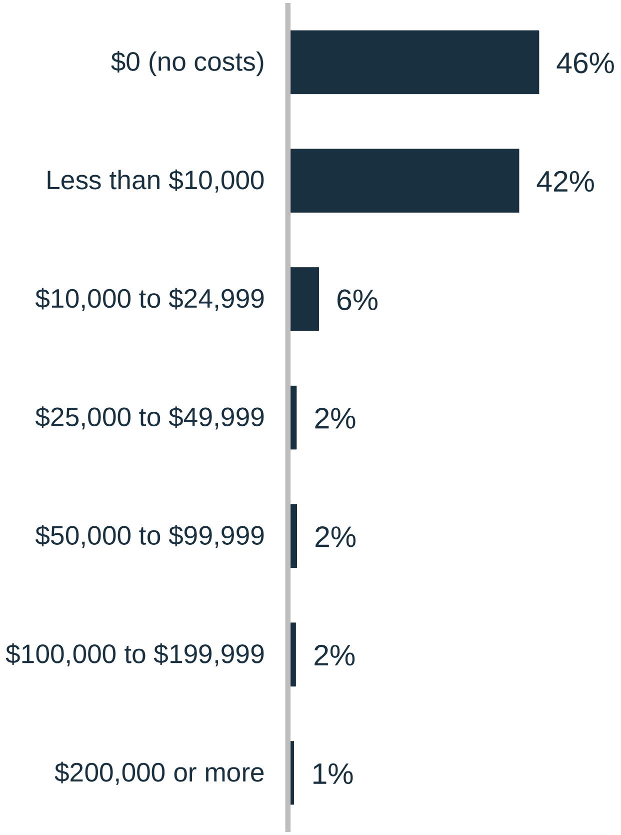
Here's a rule of thumb to determine the daily cost of not being able to do business due to disruption of operations:

$$\frac{\text{Total yearly revenue + Total yearly expenses}}{\text{Number of days in operation in a year}}$$

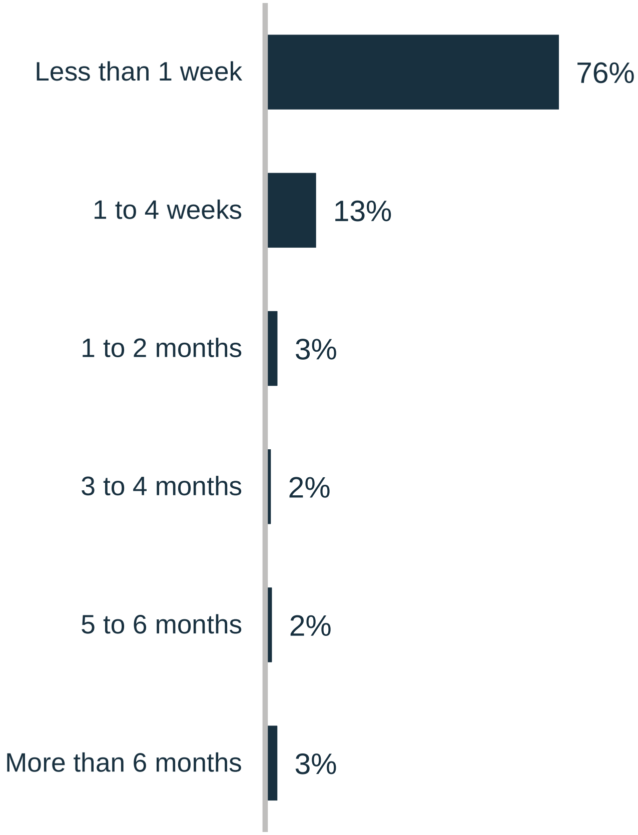
Base: Those who experienced a cybersecurity incident (n=364). Those who did not know were excluded from the calculation base. Multiple mentions were allowed, therefore total exceeds 100%.*This rule of thumb does not include professional fees, ransom, investments, nor reputational consequences.

For some SMEs, no costs were associated with the incident they experienced. For those for whom the incident had a cost, the reported costs of the incident averages slightly over $20K.

S3Q4. What were the **costs** associated with the **most recent** incident? *Include incremental costs during and after the incident (i.e., overtime, professional fees, security tool investment, insurance cost increase, etc.). Please do not include ransom costs.*



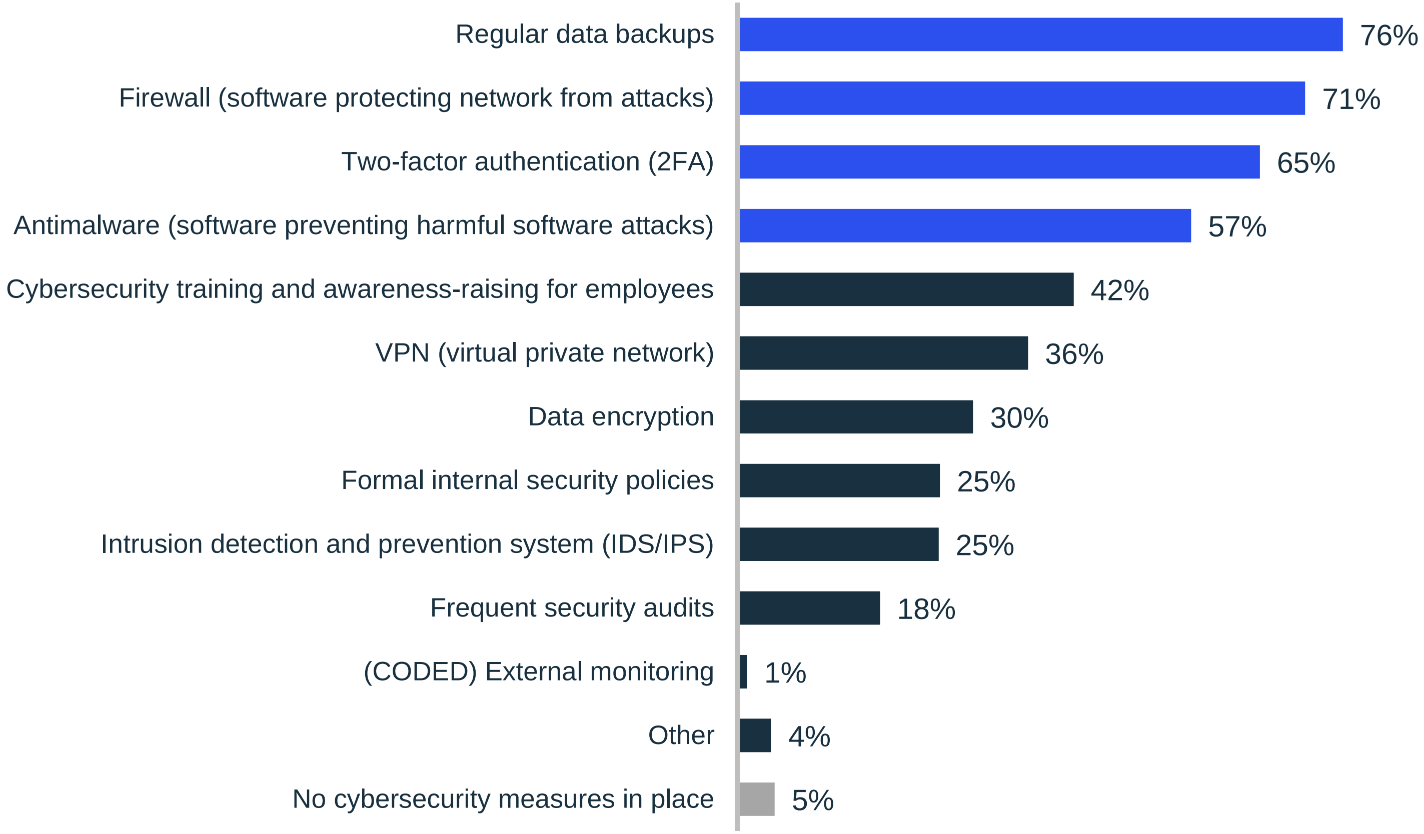
S3Q5. How **long** did it take your company to **fully recover** from the **most recent** cyberincident?



Base: Those who experienced a cybersecurity incident (n=352-360). Those who did not know were excluded from the calculation base.

While phishing is the most experienced incident, only 2 out of 5 SMEs have cybersecurity trainings in place for their employees.

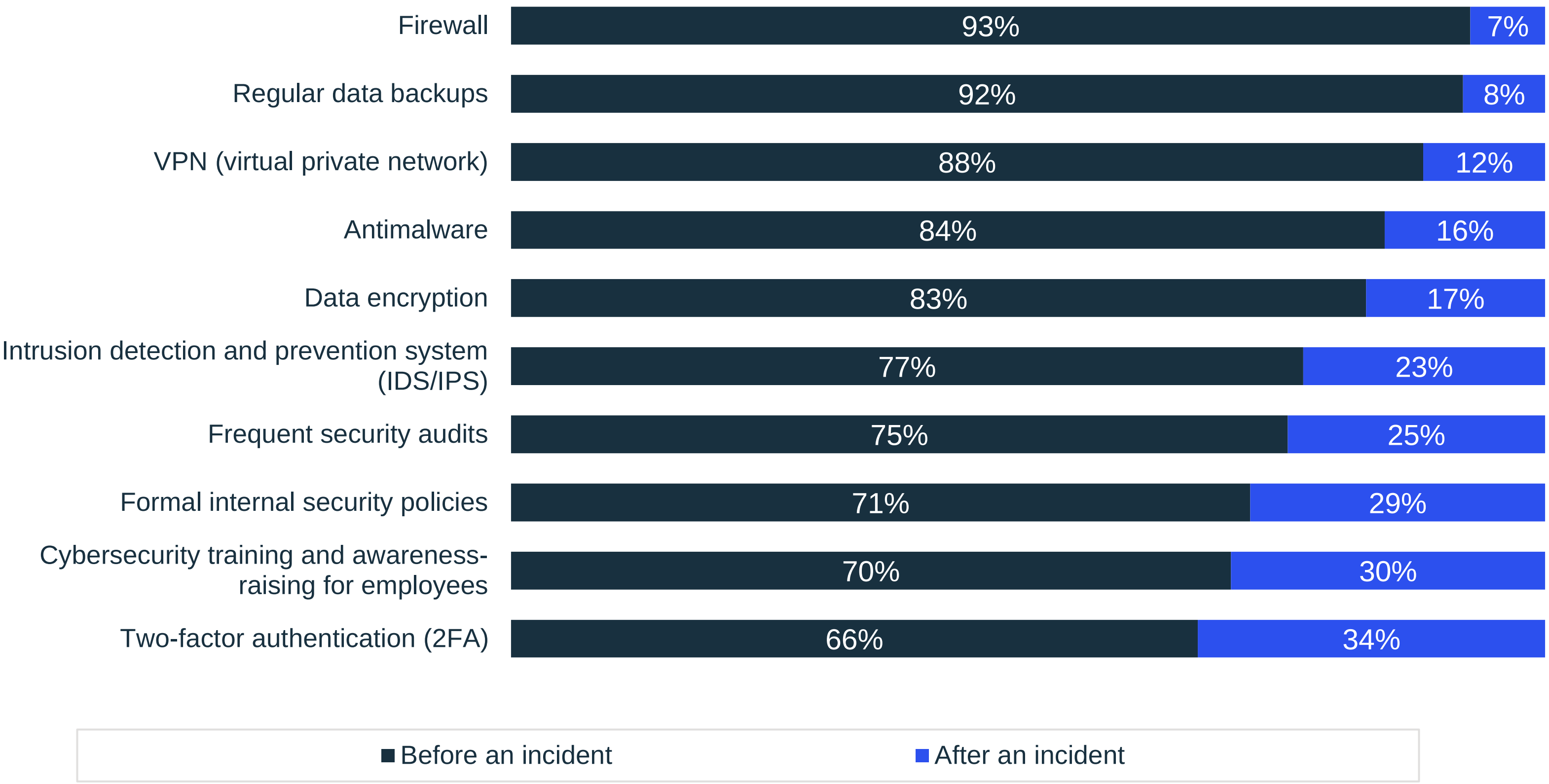
S3Q6. What cybersecurity **measures** and **tools** has your company put in place and is **currently** using?



Base: All respondents (n=484). Those who did not know or preferred not to answer were excluded from the calculation base. Multiple mentions were allowed, therefore total exceeds 100%.

Cybersecurity training and 2-factor authentication are two preventative measures that SMEs could implement to reduce user-related risks. It's not surprising to see them as measures put in place after an incident.

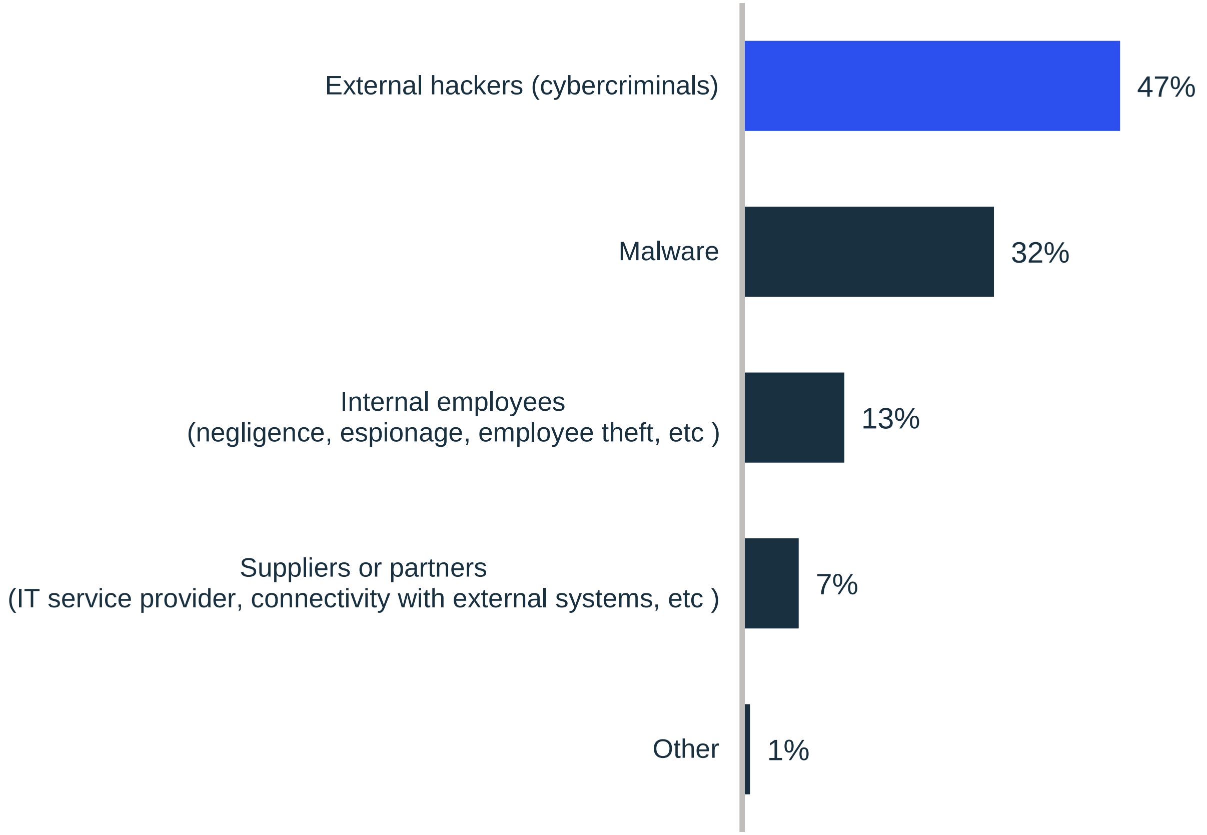
S3Q7. Were those **measures** implemented **before** or **after** a cybersecurity incident happened at your company?



Base: Those who experienced a cybersecurity incident and who have preventative measures in place (n=83-296). Those who did not know were excluded from the calculation base.

When asked to name the main source of cybersecurity threats in their business, external hackers come out on top. Employees, suppliers or partners are deemed less risky in the eyes of business owners.

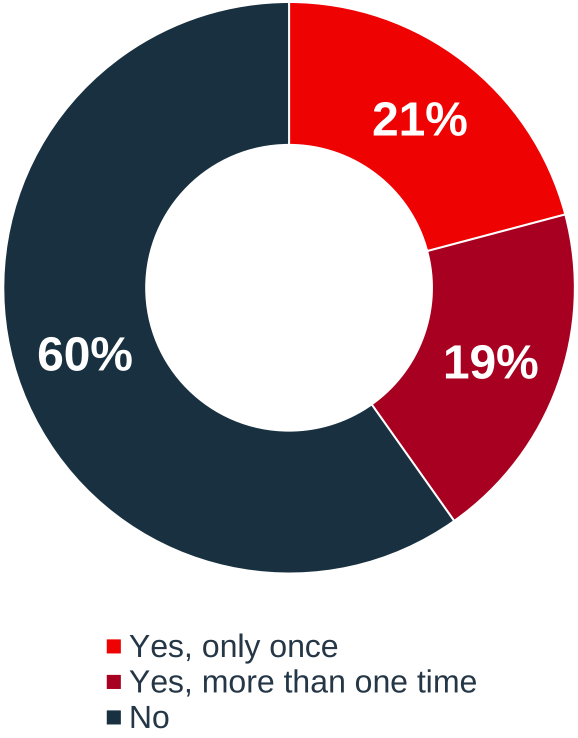
S3Q8. What do you see as the **main source of cybersecurity threats** to your company?



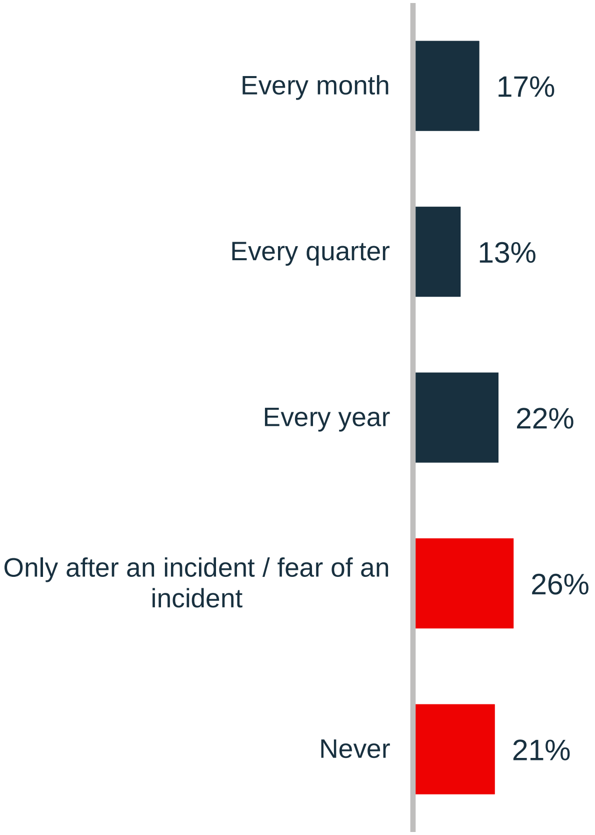
Base: All respondents (n=473). Those who did not know or preferred not to answer were excluded from the calculation base.

Two out of 5 SMEs have been impacted by an external party's incident. SMEs who have never experienced an incident are also more likely to have never assessed this type of risk.

S3Q9. Has your company ever been **indirectly impacted** by a cybersecurity incident from an **external party** (client, supplier, partner, etc.)?



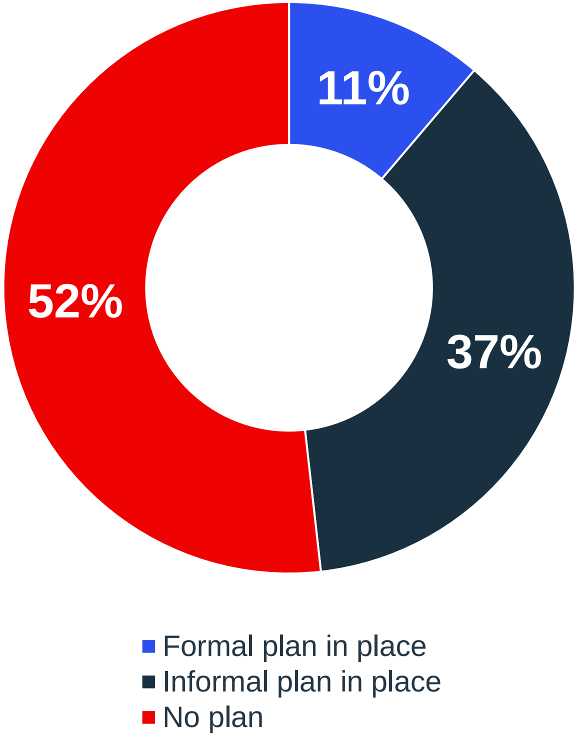
S3Q10. How **often** does your company assess the **cybersecurity risks** associated with your clients, suppliers and partners?



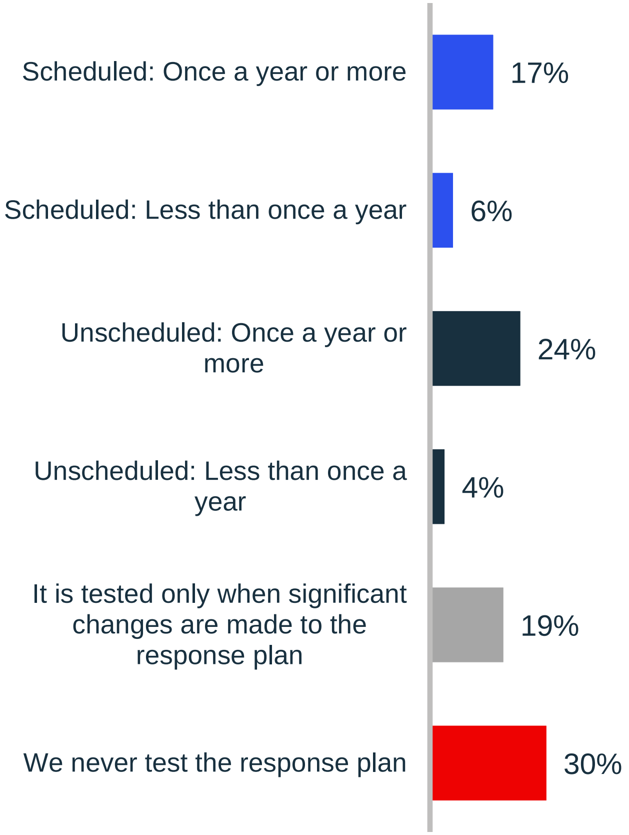
Base: All respondents (n=449-500). Those who did not know were excluded from the calculation base.

Fewer than half of SMEs have a response plan in place, and among these, 30% have never tested their plan. Those who have experienced network intrusion or data breach are more likely to have a plan in place.

S3Q11. Does your company have a cybersecurity incident **response plan** in place?



S3Q12. Are there **scheduled tests** of the cybersecurity incident **response plan** in place?

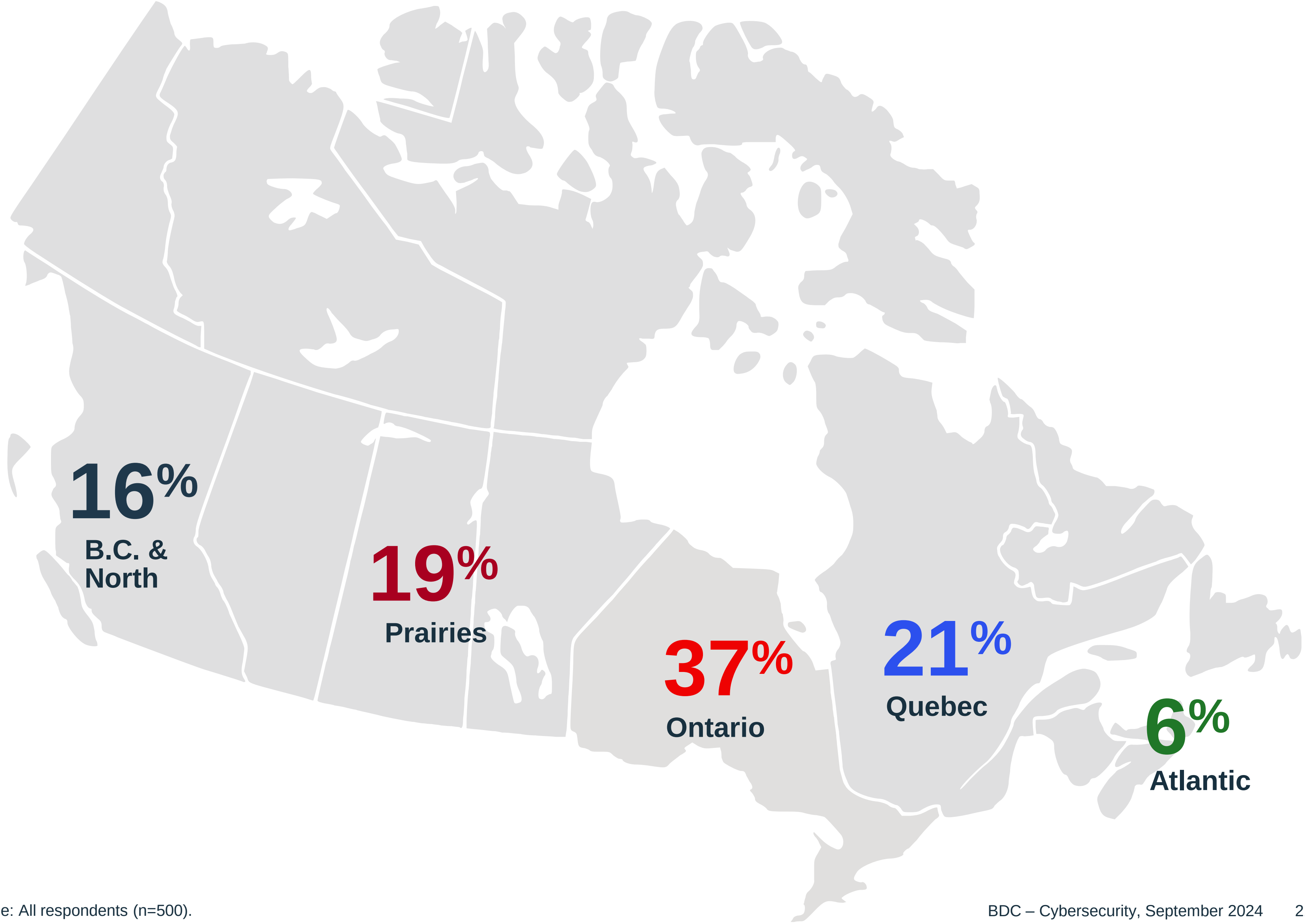


Base: S3Q11 = All respondents (n=479). S3Q12 = Those who have an incident response plan in place (n=230). Those who did not know were excluded from the calculation base.

4

Respondent profile

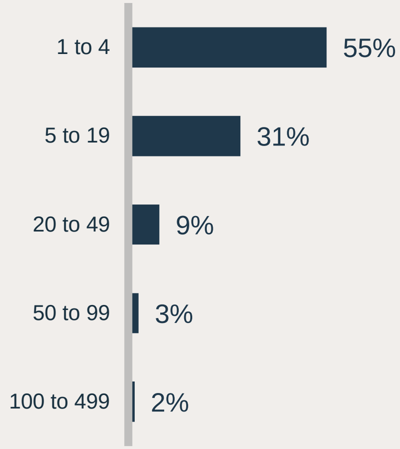
Region



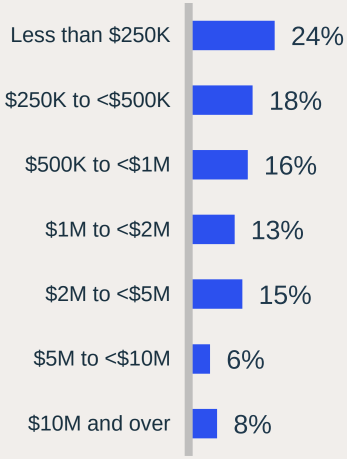
Base: All respondents (n=500).

Respondent profile

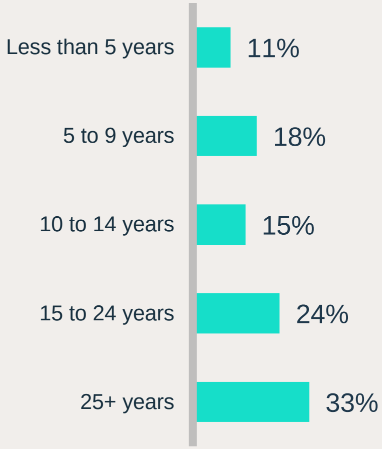
Number of employees



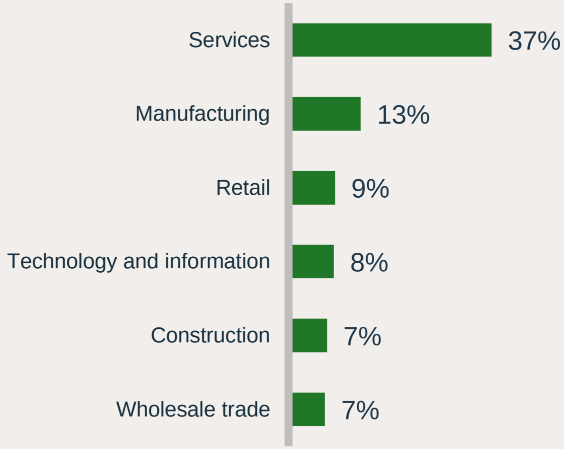
Annual sales



Years in business



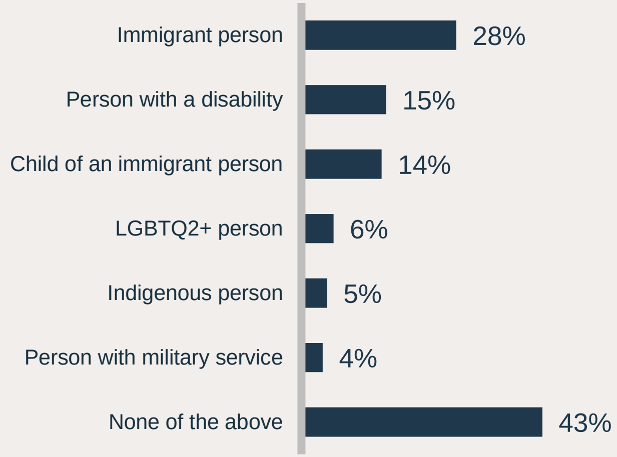
Main sector of activity



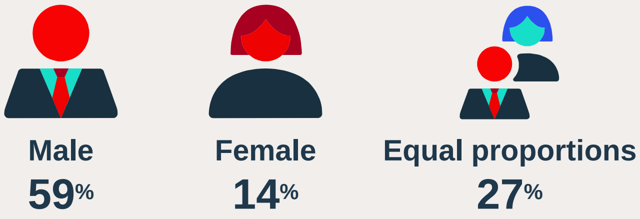
Base: All respondents (n=483-500). Those who did not know or preferred not to answer were excluded from the calculation base. For the sectors, only those with 7%+ respondents are presented.

Respondent profile

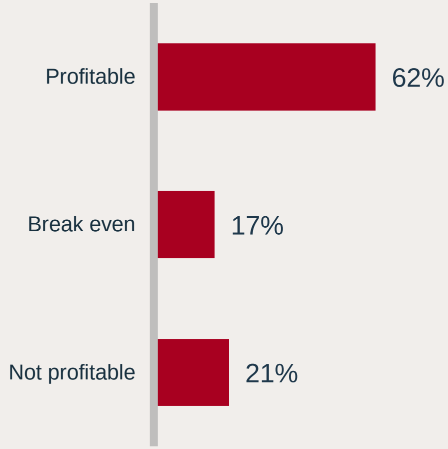
Diversity*



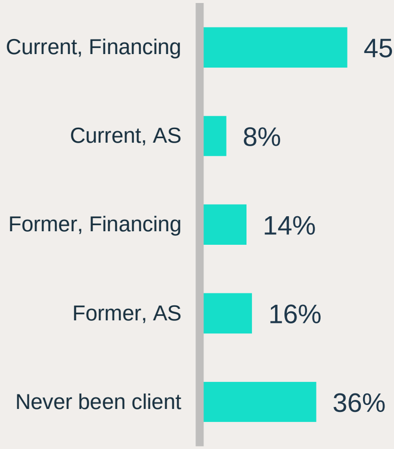
Gender ownership



Profitability



Client status*



Base: All respondents (n=457-498). Those who did not know or preferred not to answer were excluded from the calculation base. *Multiple mentions were allowed, therefore total exceeds 100%.

5

Appendix

Results by business revenue

Perceptions

S3Q1. To what extent do you **agree** with the following statements?

	Business revenue		
% of 7 to 10	**Less than $3M**	**$3M to less than <$10M**	**$10M or more**
The larger the company, the more likely it is to be targeted by a cyber attack	**63%** ↑	**48%** ↓	60%
I believe that our company has, host or use data that puts it at risk of being targeted by a cyberattack	38%	46%	47%
I am confident that my company would fully recover from a cybersecurity incident within one month	51%	49%	59%
I feel that my company is well prepared to handle a cybersecurity incident	45%	49%	**62%** ↑
Sample size	*274-285*	*102-104*	*97-99*

Base: All respondents. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample.

Past cybersecurity incidents

S3Q2. Has your company ever experienced **cybersecurity incidents** in the past?

Business revenue

	Less than $3M	$3M to less than <$10M	$10M or more
Phishing (attempted email fraud)	59%	60%	**81% ↑**
Malware (malicious software causing harm)	26%	32%	31%
Network intrusion (unauthorized access to company network)	12%	15%	8%
Ransomware (external software encrypting files for ransom)	**10% ↓**	15%	**21% ↑**
Data breach (unauthorized access to sensitive information)	6%	10%	12%
Denial-of-service attacks (DDoS) (overwhelming network to disrupt service)	5%	6%	9%
Other	2%	5%	0%
We have experienced an incident, but I don't know the type	5%	5%	0%
No cybersecurity incident in the past	28%	24%	**15% ↓**
TOTAL: Experienced past incident	**72%**	**76%**	**85% ↑**
TOTAL: Other than phishing	**40%**	**47%**	**54%**
Sample size	*290*	*103*	*101*

Base: All respondents. Those who preferred not to answer were excluded from the calculation base. Multiple mentions were allowed, therefore total exceeds 100%. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample.

Impacts of incident

S3Q3. What were the **impacts** of the **most recent** cybersecurity incident on your company?

	Business revenue		
	Less than $3M	**$3M to less than <$10M**	**$10M or more**
Disruption of operations	40%	51%	37%
Increased security costs	**20%** ↓	**34%** ↑	31%
Significant unplanned expenses	21%	20%	15%
Damage to reputation	13%	9%	**2%** ↓
Loss of sensitive data	8%	4%	4%
Loss of clients	**7%** ↑	**0%** ↓	0%
Increased insurance premiums	**3%** ↓	8%	**10%** ↑
Legal or regulatory obligations to comply to	4%	3%	6%
Other	2%	3%	2%
No impacts	45%	34%	40%
TOTAL: Had impacts	**55%**	**66%**	**60%**
Sample size	*203*	*78*	*83*

Base: Those who experienced a cybersecurity incident. Those who did not know were excluded from the calculation base. Multiple mentions were allowed, therefore total exceeds 100%. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample.

Costs of the incident

S3Q4. What were the **costs** associated with the **most recent** incident?

	Business revenue		
	Less than $3M	**$3M to less than <$10M**	**$10M or more**
$0 (no costs)	47%	42%	37%
Less than $10,000	44%	32%	36%
$10,000 to $24,999	**3% ↓**	**18% ↑**	10%
$25,000 to $49,999	**1% ↓**	**4% ↑**	3%
$50,000 to $99,999	1%	3%	3%
$100,000 to $199,999	2%	0%	2%
$200,000 or more	1%	0%	**7% ↑**
NET: $10,000 or more	**8% ↓**	**26% ↑**	**27% ↑**
Average	**$9,053**	**$9,552**	**$28,787 ↑**
Sample size	*202*	*80*	*78*

Base: Those who experienced a cybersecurity incident. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample.

Time of recovery from the incident

S3Q5. How **long** did it take your company to **fully recover** from the **most recent** cyberincident?

	Business revenue		
	Less than $3M	**$3M to less than <$10M**	**$10M or more**
Less than 1 week	76%	77%	75%
1 to 4 weeks	13%	14%	14%
1 to 2 months	3%	4%	2%
3 to 4 months	2%	1%	2%
5 to 6 months	2%	1%	1%
More than 6 months	3%	3%	6%
NET: 1 month or more	**11%**	**9%**	**11%**
Sample size	*193*	*78*	*81*

Base: Those who experienced a cybersecurity incident. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample.

Current measures and tools

S3Q6. What cybersecurity **measures** and **tools** has your company put in place and is **currently** using?

	Business revenue		
	Less than $3M	**$3M to less than <$10M**	**$10M or more**
Regular data backups	**73% ↓**	84%	**87% ↑**
Firewall (software protecting network from attacks)	**67% ↓**	**83% ↑**	**93% ↑**
Two-factor authentication (2FA)	66%	58%	71%
Antimalware (software preventing harmful software attacks)	55%	59%	67%
Cybersecurity training and awareness-raising for employees	**39% ↓**	47%	**68% ↑**
VPN (virtual private network)	**31% ↓**	**49% ↑**	**63% ↑**
Data encryption	**27% ↓**	32%	**47% ↑**
Formal internal security policies	**21% ↓**	**38% ↑**	**50% ↑**
Intrusion detection and prevention system (IDS/IPS)	**21% ↓**	**35% ↑**	**46% ↑**
Frequent security audits	**15% ↓**	23%	**35% ↑**
(CODED) External monitoring	1%	3%	2%
Other	5%	2%	6%
No cybersecurity measures in place	**6% ↑**	2%	0%
Sample size	*283*	*102*	*99*

Base: All respondents. Those who did not know or preferred not to answer were excluded from the calculation base. Multiple mentions were allowed, therefore total exceeds 100%.
Arrows indicate statistically significant differences between a given sub-group and the rest of the sample.

Moment of implementation of measures

S3Q7. Were those **measures** implemented **before** or **after** a cybersecurity incident happened at your company?

	Business revenue		
% who implemented after an incident	**Less than $3M**	**$3M to less than <$10M**	**$10M or more**
Antimalware (software preventing harmful software attacks)	17%	12%	10%
Firewall (software protecting network from attacks)	9%	5%	**1% ↓**
Intrusion detection and prevention system (IDS/IPS)	21%	26%	28%
Data encryption	19%	*18%**	6%
Two-factor authentication (2FA)	33%	40%	33%
Regular data backups	8%	11%	0%
Cybersecurity training and awareness-raising for employees	30%	29%	36%
VPN (virtual private network)	13%	13%	3%
Frequent security audits	16%	*42%**	*37%**
Formal internal security policies	28%	33%	26%
Sample size	*30-149*	*25-72*	*28-78*

Base: Those victims of a cybersecurity incident who have measures in place. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution.

Main cybersecurity threat

S3Q8. What do you see as the **main source of cybersecurity threats** to your company?

	Business revenue		
	Less than $3M	**$3M to less than <$10M**	**$10M or more**
External hackers (cybercriminals)	47%	48%	53%
Malware	**34% ↑**	25%	**19% ↓**
Internal employees (negligence, espionage, employee theft, etc.)	**11% ↓**	20%	**24% ↑**
Suppliers or partners (IT service provider, connectivity with external systems, etc.)	8%	5%	2%
Other	1%	2%	3%
Sample size	*272*	*102*	*99*

Base: All respondents. Those who did not know or preferred not to answer were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample.

Indirect cybersecurity incident

S3Q9. Has your company ever been **indirectly impacted** by a cybersecurity incident from an **external party** (client, supplier, partner, etc.)?

	Business revenue		
	Less than $3M	**$3M to less than <$10M**	**$10M or more**
Yes, only once	21%	18%	22%
Yes, more than one time	**17% ↓**	20%	**37% ↑**
No	61%	62%	**42% ↓**
NET: Yes	**39%**	**38%**	**58% ↑**
Sample size	*262*	*96*	*91*

Base: All respondents. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample.

Risk assessment of external parties

S3Q10. How **often** does your company assess the **cybersecurity risks** associated with your clients, suppliers and partners?

	Business revenue		
	Less than $3M	**$3M to less than <$10M**	**$10M or more**
Every month	18%	**10%** ↓	22%
Every quarter	12%	18%	14%
Every year	22%	22%	25%
Only after an incident / fear of an incident	26%	25%	30%
Never	22%	25%	**8%** ↓
Sample size	*263*	*88*	*87*

Base: All respondents. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample.

Response plan in place

S3Q11. Does your company have a cybersecurity incident **response plan** in place?

	Business revenue		
	Less than $3M	**$3M to less than <$10M**	**$10M or more**
Yes, we have a formal plan	**8% ↓**	**20% ↑**	**32% ↑**
Yes, we have an informal plan	38%	27%	40%
No	54%	53%	**29% ↓**
NET: Yes	**46%**	**47%**	**71% ↑**
Sample size	*285*	*99*	*95*

Base: All respondents. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample.

Tests of the response plan

S3Q12. Are there **scheduled tests** of the cybersecurity incident **response plan** in place?

	Business revenue		
	Less than $3M	**$3M to less than <$10M**	**$10M or more**
Scheduled: Once a year or more	16%	17%	20%
Scheduled: Less than once a year	7%	7%	2%
Unscheduled: Once a year or more	24%	24%	21%
Unscheduled: Less than once a year	**2% ↓**	8%	**11% ↑**
It is tested only when significant changes are made to the response plan	19%	20%	23%
We never test the response plan	32%	24%	24%
TOTAL: Scheduled tests in place	**23%**	**24%**	**22%**
TOTAL: Unscheduled tests in place	**26%**	**32%**	**31%**
Sample size	*126*	*45*	*59*

Base: Those who have an incident response plan in place. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample.

5

Appendix

Results by the type of cybersecurity incident experienced

Perceptions

S3Q1. To what extent do you **agree** with the following statements?

	Type of incident							
% of 7 to 10	**Phishing**	**Malware**	**Ransom-ware**	**Network intrusion**	**Data breach**	**Denial-of-service attacks (DDoS)***	**No incident in the past**	**TOTAL: Experienced past incident**
The larger the company, the more likely it is to be targeted by a cyber attack	63%	65%	64%	61%	56%	*76%*	54%	63%
I believe that our company has, host or use data that puts it at risk of being targeted by a cyberattack	41%	43%	49%	**67% ↑**	**65% ↑**	*58%*	35%	42%
I am confident that my company would fully recover from a cybersecurity incident within one month	48%	44%	63%	41%	46%	*64%*	61%	49%
I feel that my company is well prepared to handle a cybersecurity incident	44%	39%	49%	42%	37%	***74% ↑***	55%	**44% ↓**
Sample size	*300-308*	*134-138*	*70-71*	*63-65*	*37-39*	*28*	*112-116*	*358-367*

Base: All respondents. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution. Results are not presented when sample size is smaller than 20 respondents.

Past cybersecurity incidents

S3Q2. Has your company ever experienced **cybersecurity incidents** in the past?

	Type of incident							
	Phishing	Malware	Ransom-ware	Network intrusion	Data breach	Denial-of-service attacks (DDoS)*	No incident in the past	TOTAL: Experienced past incident
Phishing (attempted email fraud)	100% ↑	90% ↑	73%	81% ↑	85% ↑	73%	0% ↓	84% ↑
Malware (malicious software causing harm)	40% ↑	100% ↑	49% ↑	50% ↑	41%	44%	0% ↓	37% ↑
Network intrusion (unauthorized access to company network)	16% ↑	21% ↑	33% ↑	100% ↑	44% ↑	33% ↑	0% ↓	16% ↑
Ransomware (external software encrypting files for ransom)	14%	21% ↑	100% ↑	32% ↑	24% ↑	40% ↑	0% ↓	16% ↑
Data breach (unauthorized access to sensitive information)	10% ↑	11%	15% ↑	27% ↑	100% ↑	14%	0% ↓	10% ↑
Denial-of-service attacks (DDoS) (overwhelming network to disrupt service)	6%	9%	18% ↑	15% ↑	10%	100% ↑	0% ↓	7% ↑
Other, please specify	3%	2%	3%	4%	5%	3%	0%	3%
We have experienced an incident, but I don't know the type	0% ↓	0% ↓	0%	0%	0%	0%	0% ↓	6% ↑
No cybersecurity incident in the past	0% ↓	0% ↓	0% ↓	0% ↓	0% ↓	0% ↓	100% ↑	0% ↓
TOTAL: Experienced past incident	100% ↑	100% ↑	100% ↑	100% ↑	100% ↑	100% ↑	0% ↓	100% ↑
Sample size	*313*	*140*	*72*	*65*	*39*	*28*	*120*	*374*

Base: All respondents. Those who preferred not to answer were excluded from the calculation base. Multiple mentions were allowed, therefore total exceeds 100%. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution. Results are not presented when sample size is smaller than 20 respondents.

Impacts of incident

S3Q3. What were the **impacts** of the **most recent** cybersecurity incident on your company?

	Type of incident							
	Phishing	Malware	Ransom-ware	Network intrusion	Data breach	Denial-of-service attacks (DDoS)*	No incident in the past	TOTAL: Experienced past incident
Disruption of operations	**36% ↓**	**56% ↑**	**81% ↑**	**69% ↑**	**66% ↑**	***89% ↑***	-	41%
Increased security costs	25%	**40% ↑**	**41% ↑**	**42% ↑**	**40% ↑**	***46% ↑***	-	23%
Significant unplanned expenses	**18% ↓**	**34% ↑**	**43% ↑**	**50% ↑**	**45% ↑**	***47% ↑***	-	20%
Damage to reputation	12%	16%	9%	**21% ↑**	20%	*18%*	-	11%
Loss of sensitive data	6%	**11% ↑**	**15% ↑**	**25% ↑**	**21% ↑**	*15%*	-	7%
Loss of clients	**3% ↓**	7%	7%	12%	9%	*8%*	-	5%
Increased insurance premiums	4%	6%	4%	**10% ↑**	**26% ↑**	*11%*	-	4%
Legal or regulatory obligations to comply to	**2% ↓**	4%	8%	**13% ↑**	**20% ↑**	*8%*	-	4%
Other	2%	3%	**7% ↑**	**7% ↑**	5%	*0%*	-	2%
No impacts	**48% ↑**	**25% ↓**	**16% ↓**	**16% ↓**	**4% ↓**	***10% ↓***	-	43%
TOTAL: Had impacts	**52% ↓**	**75% ↑**	**84% ↑**	**84% ↑**	**96% ↑**	***90% ↑***	**-**	**57%**
Sample size	*304*	*138*	*71*	*65*	*39*	*27*	*0*	*364*

Base: Those who experienced a cybersecurity incident. Those who did not know were excluded from the calculation base. Multiple mentions were allowed, therefore total exceeds 100%. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution. Results are not presented when sample size is smaller than 20 respondents.

Costs of the incident

S3Q4. What were the **costs** associated with the **most recent** incident?

Type of incident

	Phishing	Malware	Ransom-ware	Network intrusion	Data breach	Denial-of-service attacks (DDoS)*	No incident in the past	TOTAL: Experienced past incident
$0 (no costs)	**51% ↑**	**26% ↓**	**16% ↓**	32%	**5% ↓**	*27%*	-	46%
Less than $10,000	**38% ↓**	**58% ↑**	**60% ↑**	45%	45%	***66% ↑***	-	42%
$10,000 to $24,999	6%	9%	**12% ↑**	10%	**21% ↑**	*5%*	-	6%
$25,000 to $49,999	**1% ↓**	2%	4%	3%	5%	*3%*	-	2%
$50,000 to $99,999	1%	4%	3%	4%	**10% ↑**	*0%*	-	2%
$100,000 to $199,999	1%	2%	1%	4%	**9% ↑**	*0%*	-	2%
$200,000 or more	2%	0%	4%	2%	5%	*0%*	-	1%
NET: $10,000 or more	**10% ↓**	**17%**	**25% ↑**	**23% ↑**	**50% ↑**	***8%***	**-**	**12%**
Average	**$9,500**	**$11,5478**	**$21,291**	**$19,165**	**$41,103 ↑**	***$5,133 ↓***	**-**	**$10,907**
Sample size	*301*	*136*	*70*	*61*	*37*	*25*	*0*	*360*

Base: Those who experienced a cybersecurity incident. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution. Results are not presented when sample size is smaller than 20 respondents.

Time of recovery from the incident

S3Q5. How **long** did it take your company to **fully recover** from the **most recent** cyberincident?

Type of incident

	Phishing	Malware	Ransom-ware	Network intrusion	Data breach	Denial-of-service attacks (DDoS)*	No incident in the past	TOTAL: Experienced past incident
Less than 1 week	**79% ↑**	**65% ↓**	**57% ↓**	**64% ↓**	**39% ↓**	*62%*	-	76%
1 to 4 weeks	12%	**19% ↑**	**25% ↑**	15%	**34% ↑**	*11%*	-	13%
1 to 2 months	3%	5%	5%	6%	5%	*12%*	-	3%
3 to 4 months	1%	3%	**5% ↑**	0%	0%	*0%*	-	2%
5 to 6 months	2%	3%	4%	**8% ↑**	5%	*8%*	-	2%
More than 6 months	2%	5%	4%	8%	**17% ↑**	*7%*	-	3%
NET: 1 month or more	**9% ↓**	**15%**	**18%**	**21% ↑**	**27% ↑**	**27% ↑**	**-**	**11%**
Sample size	*294*	*138*	*71*	*62*	*37*	*27*	*0*	*352*

Base: Those who experienced a cybersecurity incident. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution. Results are not presented when sample size is smaller than 20 respondents.

Current measures and tools

S3Q6. What cybersecurity **measures** and **tools** has your company put in place and is **currently** using?

Type of incident

	Phishing	Malware	Ransom-ware	Network intrusion	Data breach	Denial-of-service attacks (DDoS)*	No incident in the past	TOTAL: Experienced past incident
Regular data backups	77%	80%	80%	79%	75%	*92%*	77%	75%
Firewall (software protecting network from attacks)	72%	75%	76%	80%	72%	*92%*	70%	71%
Two-factor authentication (2FA)	68%	**74% ↑**	66%	66%	63%	*61%*	65%	65%
Antimalware (software preventing harmful software attacks)	58%	**66% ↑**	46%	49%	57%	*68%*	57%	57%
Cybersecurity training and awareness-raising for employees	44%	41%	49%	52%	50%	*61%*	42%	42%
VPN (virtual private network)	38%	37%	31%	43%	41%	*56%*	35%	37%
Data encryption	31%	36%	39%	40%	46%	***75% ↑***	24%	31%
Formal internal security policies	**29% ↑**	31%	35%	35%	36%	***53% ↑***	20%	27%
Intrusion detection and prevention system (IDS/IPS)	25%	21%	24%	19%	38%	***49% ↑***	25%	25%
Frequent security audits	19%	17%	**33% ↑**	28%	22%	***44% ↑***	14%	19%
(CODED) External monitoring	1%	1%	0%	0%	6%	*0%*	1%	1%
Other	5%	3%	7%	4%	4%	***19% ↑***	4%	4%
No cybersecurity measures in place	4%	**0% ↓**	0%	5%	5%	*0%*	6%	4%
Sample size	*311*	*139*	*70*	*65*	*39*	*27*	*114*	*368*

Base: All respondents. Those who did not know or preferred not to answer were excluded from the calculation base. Multiple mentions were allowed, therefore total exceeds 100%. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution. Results are not presented when sample size is smaller than 20 respondents.

Moment of implementation of measures

S3Q7. Were those **measures** implemented **before** or **after** a cybersecurity incident happened at your company?

Type of incident

% who implemented after an incident	Phishing	Malware	Ransom ware*	Network intrusion*	Data breach*	Denial-of-service attacks (DDoS)*	No incident in the past	TOTAL: Experienced past incident
Antimalware (software preventing harmful software attacks)	**13% ↓**	19%	20%	16%	30%	5%	-	16%
Firewall (software protecting network from attacks)	6%	8%	13%	7%	3%	6%*	-	7%
Intrusion detection and prevention system (IDS/IPS)	19%	34%	43%*	26%*	n/a	n/a	-	24%
Data encryption	17%	**29% ↑**	29%*	26%*	n/a	n/a	-	17%
Two-factor authentication (2FA)	33%	40%	**55% ↑**	**53% ↑**	**67% ↑**	n/a	-	34%
Regular data backups	8%	11%	15%	9%	20%	13%*	-	8%
Cybersecurity training and awareness-raising for employees	32%	**45% ↑**	44%	33%	**54% ↑**	n/a	-	30%
VPN (virtual private network)	**7% ↓**	18%	**28% ↑**	8%	n/a	n/a	-	12%
Frequent security audits	25%	39%	43%*	30%*	n/a	n/a	-	25%
Formal internal security policies	27%	39%	48%*	42%*	n/a	n/a	-	29%
Sample size	70-256	31-117	23-59	20-56	14-30	15-26	0	82-295

Base: Those victims of a cybersecurity incident who have measures in place. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution. Results are not presented when sample size is smaller than 20 respondents.

Main cybersecurity threat

S3Q8. What do you see as the **main source of cybersecurity threats** to your company?

	Type of incident							
	Phishing	**Malware**	**Ransom-ware**	**Network intrusion**	**Data breach**	**Denial-of-service attacks (DDoS)***	**No incident in the past**	**TOTAL: Experienced past incident**
External hackers (cybercriminals)	46%	47%	58%	59%	63%	*60%*	46%	48%
Malware	33%	39%	25%	26%	20%	*20%*	28%	33%
Internal employees (negligence, espionage, employee theft, etc.)	13%	**7% ↓**	15%	7%	8%	*15%*	13%	12%
Suppliers or partners (IT service provider, connectivity with external systems, etc.)	7%	6%	**1% ↓**	9%	8%	*0%*	10%	6%
Other	1%	1%	0%	0%	0%	*5%*	2%	1%
Sample size	*306*	*139*	*69*	*62*	*37*	*26*	*108*	*362*

Base: All respondents. Those who did not know or preferred not to answer were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution. Results are not presented when sample size is smaller than 20 respondents.

Indirect cybersecurity incident

S3Q9. Has your company ever been **indirectly impacted** by a cybersecurity incident from an **external party** (client, supplier, partner, etc.)?

	Type of incident							
	Phishing	Malware	Ransom-ware	Network intrusion	Data breach	Denial-of-service attacks (DDoS)*	No incident in the past	TOTAL: Experienced past incident
Yes, only once	21%	22%	**34% ↑**	29%	32%	*35%*	**11% ↓**	**24% ↑**
Yes, more than one time	**27% ↑**	**34% ↑**	**33% ↑**	**40% ↑**	**46% ↑**	*27%*	**7% ↓**	**24% ↑**
No	**52% ↓**	**45% ↓**	**33% ↓**	**32% ↓**	**22% ↓**	*38%*	**82% ↑**	**51% ↓**
NET: Yes	**48% ↑**	**55% ↑**	**67% ↑**	**68% ↑**	**78% ↑**	***62%***	**18% ↓**	**49% ↑**
Sample size	*279*	*127*	*66*	*54*	*33*	*24*	*114*	*333*

Base: All respondents. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution. Results are not presented when sample size is smaller than 20 respondents.

Risk assessment of external parties

S3Q10. How **often** does your company assess the **cybersecurity risks** associated with your clients, suppliers and partners?

	Type of incident							
	Phishing	**Malware**	**Ransom-ware**	**Network intrusion**	**Data breach**	**Denial-of-service attacks (DDoS)***	**No incident in the past**	**TOTAL: Experienced past incident**
Every month	17%	12%	25%	28%	24%	***38% ↑***	16%	18%
Every quarter	11%	15%	20%	8%	8%	*23%*	13%	13%
Every year	21%	21%	25%	25%	24%	*32%*	22%	23%
Only after an incident / fear of an incident	**33% ↑**	**39% ↑**	23%	24%	38%	***2% ↓***	**16% ↓**	**29% ↑**
Never	18%	**13% ↓**	**8% ↓**	15%	**7% ↓**	***6% ↓***	**34% ↑**	**17% ↓**
Sample size	*277*	*127*	*63*	*56*	*37*	*24*	*105*	*331*

Base: All respondents. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution. Results are not presented when sample size is smaller than 20 respondents.

Response plan in place

S3Q11. Does your company have a cybersecurity incident **response plan** in place?

	Type of incident							
	Phishing	**Malware**	**Ransom-ware**	**Network intrusion**	**Data breach**	**Denial-of-service attacks (DDoS)***	**No incident in the past**	**TOTAL: Experienced past incident**
Yes, we have a formal plan	13%	13%	17%	**25% ↑**	**27% ↑**	*24%*	7%	13%
Yes, we have an informal plan	38%	37%	41%	35%	35%	*40%*	33%	39%
No	49%	50%	43%	39%	38%	*36%*	60%	49%
NET: Yes	**51%**	**50%**	**57%**	**61%**	**62%**	***64%***	**40%**	**51%**
Sample size	*302*	*137*	*71*	*62*	*39*	*28*	*117*	*360*

Base: All respondents. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution. Results are not presented when sample size is smaller than 20 respondents.

Tests of the response plan

S3Q12. Are there **scheduled tests** of the cybersecurity incident **response plan** in place?

Type of incident

	Phishing	**Malware**	**Ransom-ware**	**Network intrusion**	**Data breach***	**Denial-of-service attacks (DDoS)***	**No incident in the past**	**TOTAL: Experienced past incident**
Scheduled: Once a year or more	**12% ↓**	**7% ↓**	22%	21%	*17%*	*n/a*	21%	15%
Scheduled: Less than once a year	5%	7%	8%	2%	*8%*	*n/a*	9%	5%
Unscheduled: Once a year or more	26%	**42% ↑**	38%	38%	*38%*	*n/a*	19%	25%
Unscheduled: Less than once a year	**5% ↑**	4%	**1% ↓**	3%	*6%*	*n/a*	2%	5%
It is tested only when significant changes are made to the response plan	18%	**8% ↓**	21%	21%	*12%*	*n/a*	24%	18%
We never test the response plan	33%	32%	**11% ↓**	**15% ↓**	*20%*	*n/a*	25%	32%
TOTAL: Scheduled tests in place	**17% ↓**	**14%**	**30%**	**23%**	***25%***	*n/a*	**31%**	**21%**
TOTAL: Unscheduled tests in place	**31%**	**46% ↑**	**38%**	**41%**	***44%***	*n/a*	**20%**	**29%**
Sample size	*151*	*67*	*40*	*38*	*22*	*16*	*48*	*181*

Base: Those who have an incident response plan in place. Those who did not know were excluded from the calculation base. Arrows indicate statistically significant differences between a given sub-group and the rest of the sample. *Sample size is small, please interpret with caution. Results are not presented when sample size is smaller than 20 respondents.

Thank you.

Research and market intelligence team

bdc