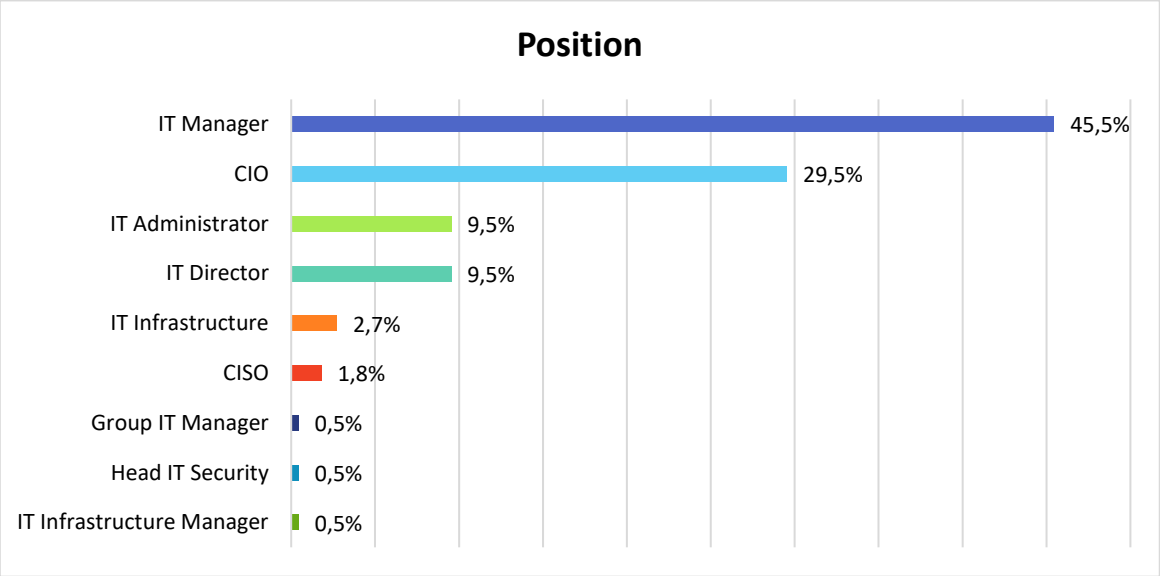
The State of Enterprise Security in South Africa 2019

Research conducted by World Wide Worx in partnership with VMware and Trend Micro

Contents

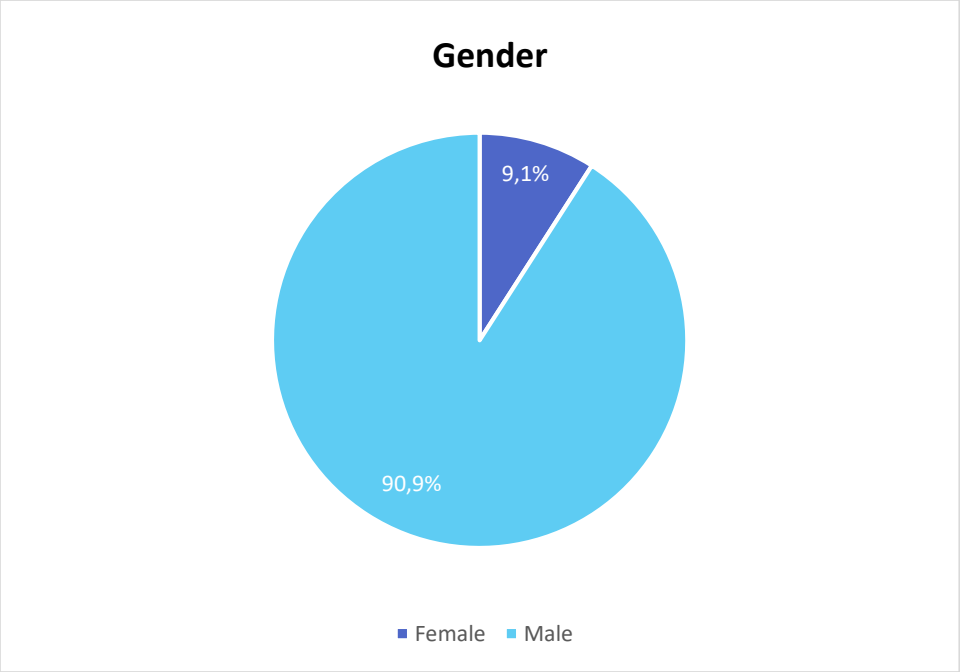
Demographics

Position



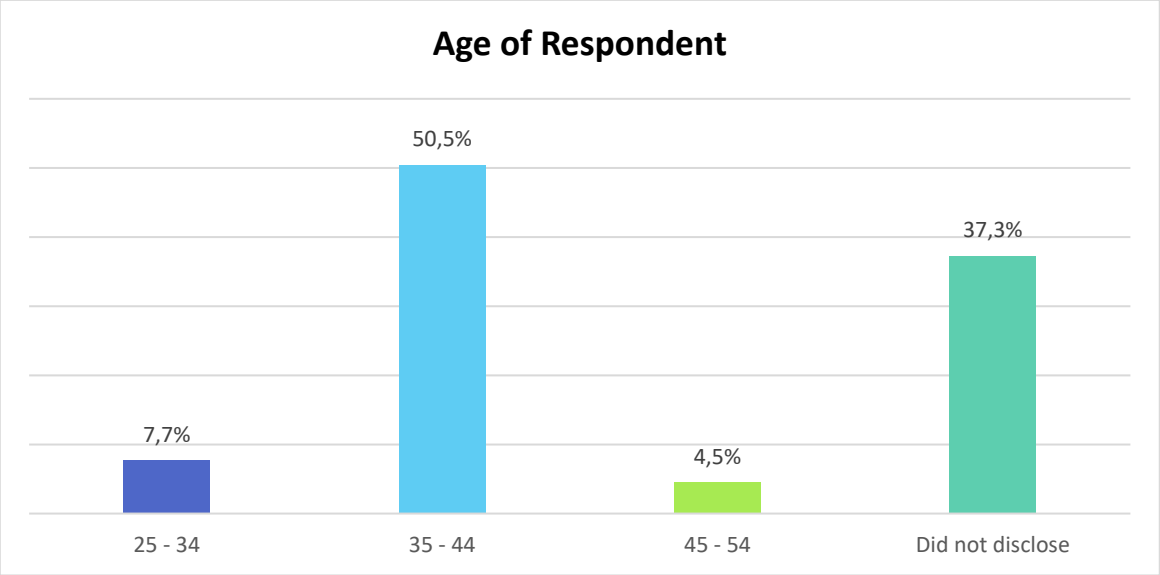
Position	Response (%)
IT Manager	45.5%
CIO	29.5%
IT Administrator	9.5%
IT Director	9.5%
IT Infrastructure	2.7%
CISO	1.8%
Group IT Manager	0.5%
Head IT Security	0.5%
IT Infrastructure Manager	0.5%

Gender



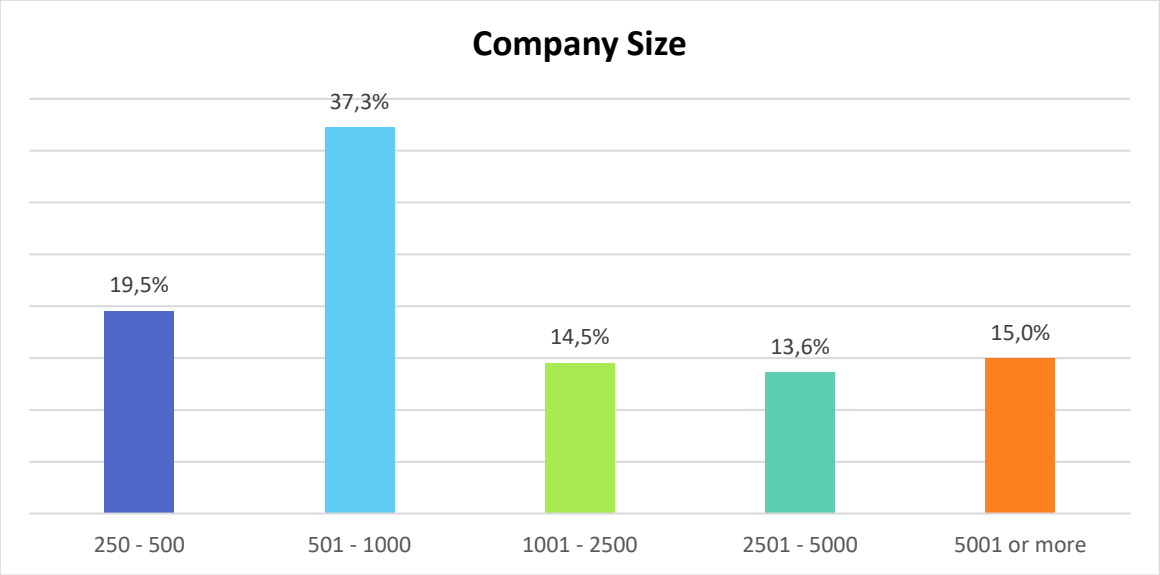
Position	Response (%)
Female	9.1%
Male	90.9%

Age of Respondent



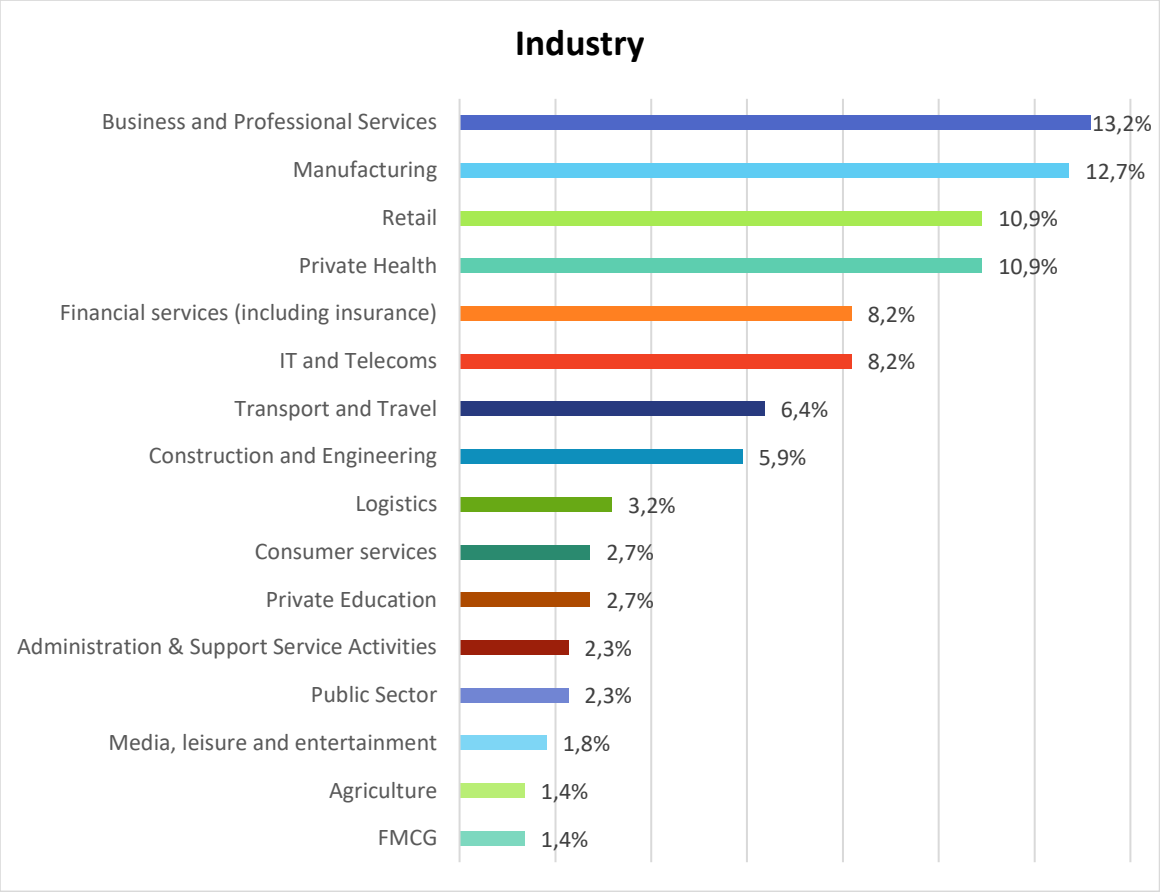
Position	Response (%)
25 - 34	7.7%
35 - 44	50.5%
45 - 54	4.5%
Did not disclose	37.3%

Company Size



Position	Response (%)
250 - 500	19.5%
501 - 1000	37.3%
1001 - 2500	14.5%
2501 - 5000	13.6%
5001 or more	15.0%

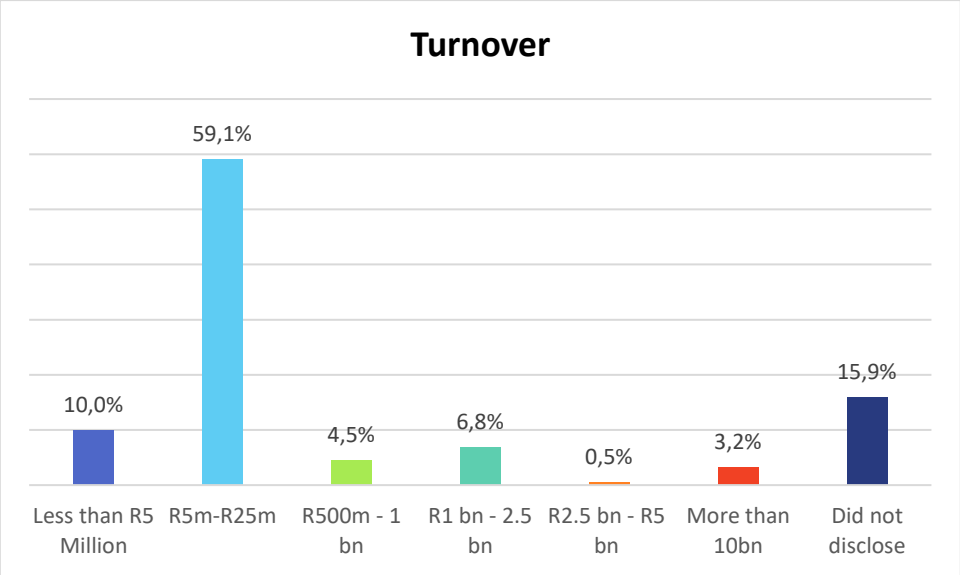
Industry



Industry	Response (%)
Business and Professional Services	13.2%
Manufacturing	12.7%
Retail	10.9%
Private Health	10.9%
Financial services (including insurance)	8.2%
IT and Telecoms	8.2%
Transport and Travel	6.4%
Construction and Engineering	5.9%
Logistics	3.2%
Consumer services	2.7%
Private Education	2.7%
Administration & Support Service Activities	2.3%
Public Sector	2.3%
Media, leisure and entertainment	1.8%
Agriculture	1.4%
FMCG	1.4%
Automotive	0.9%
Engineering & Construction	0.9%
Other	0.9%

Real Estate	0.9%
Chemicals & Pharmaceutical	0.5%
Healthcare	0.5%
Legal	0.5%
Transportation	0.5%
Utilities & Energy Services	0.5%

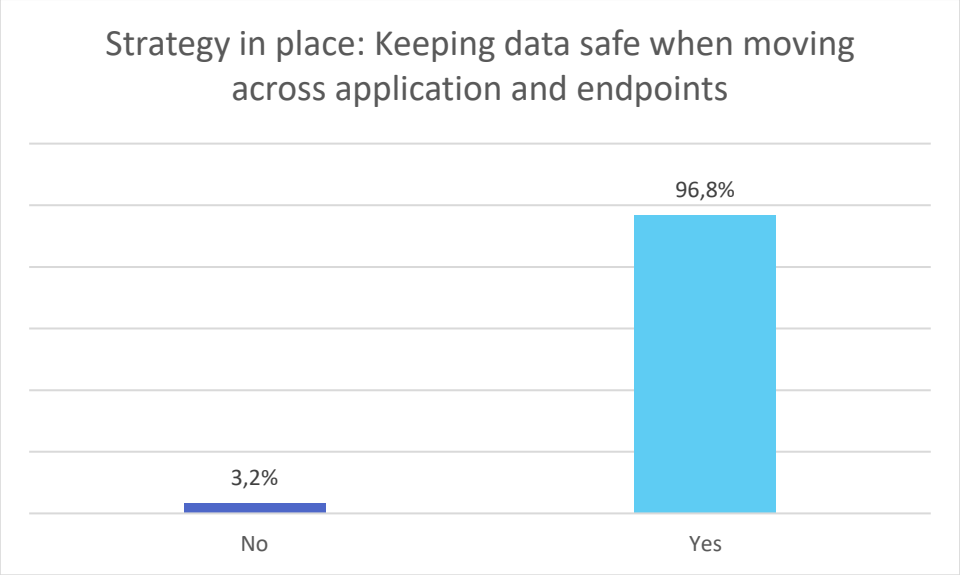
Turnover



Turnover	Response (%)
Less than R5 Million	10.0%
R5m-R25m	59.1%
R500m - 1 bn	4.5%
R1 bn - 2.5 bn	6.8%
R2.5 bn - R5 bn	0.5%
More than 10bn	3.2%
Did not disclose	15.9%

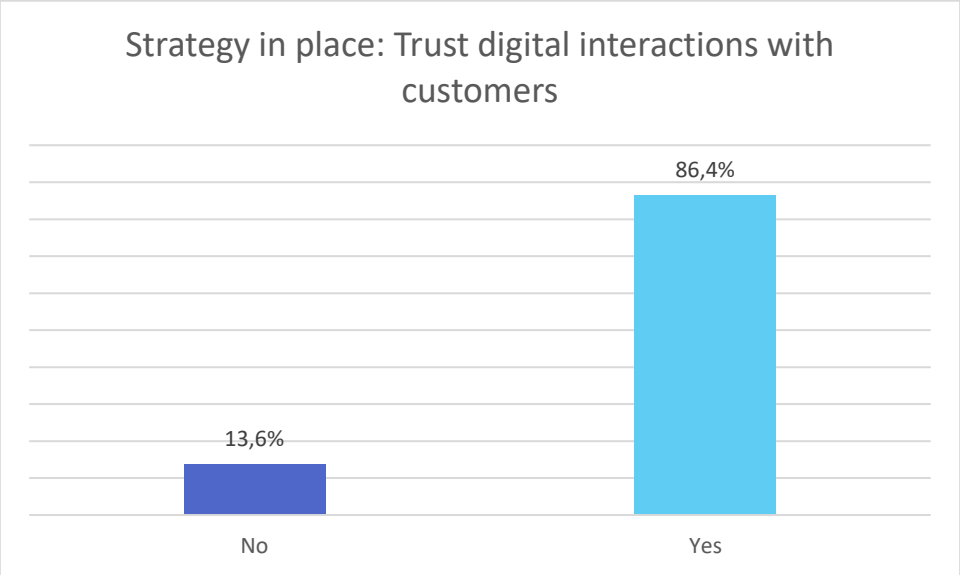
Business Strategy

Does your business have a strategy in place to support: Keeping data safe when moving across application and endpoints?



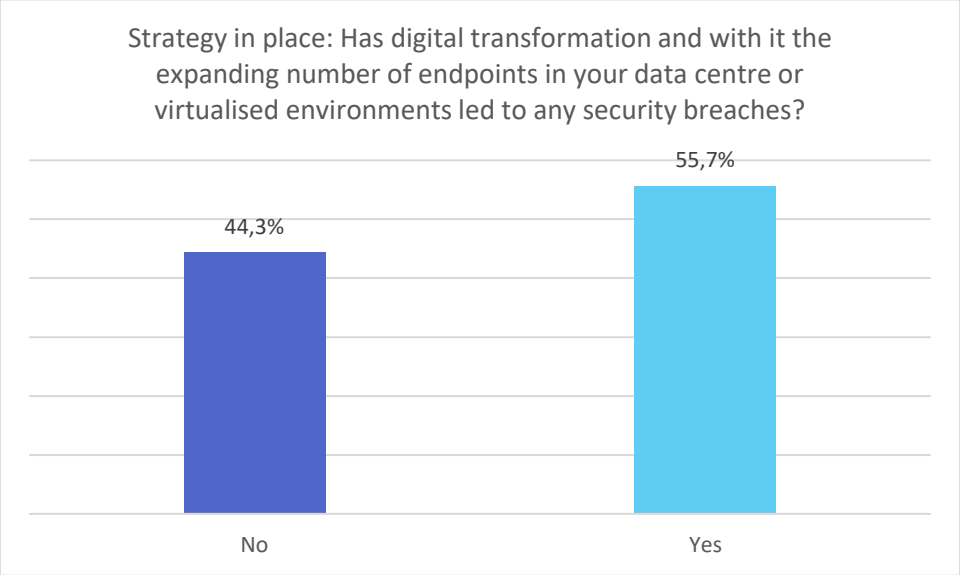
Strategy in place: Keeping data safe when moving across application and endpoints	Response (%)
Yes	96.8%
No	3.2%

Does your business have a strategy in place to support: A mechanism by which to trust digital interactions with customers?



Strategy in place: Trust digital interactions with customers	Response (%)
Yes	86.4%
No	13.6%

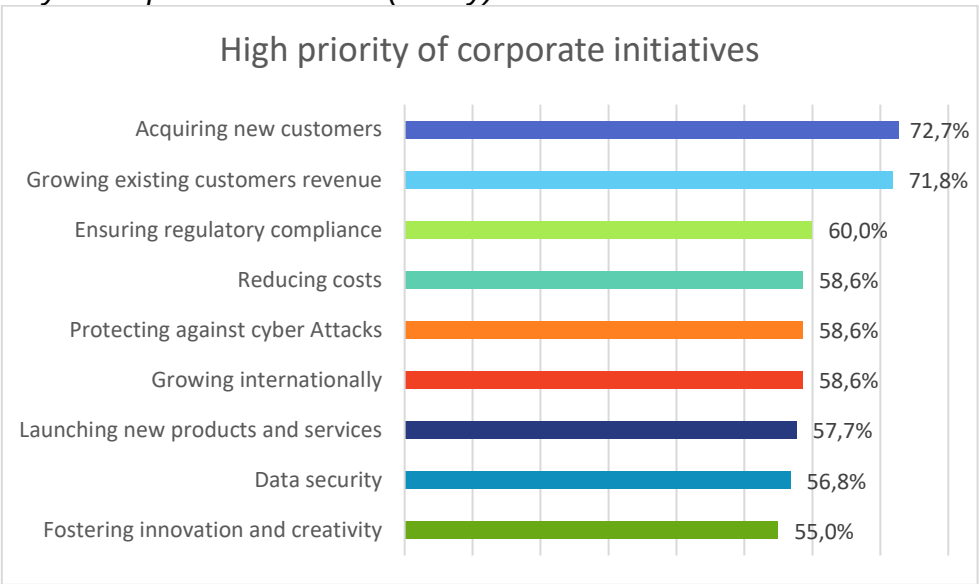
Does your business have a strategy in place to support: Has digital transformation and with it the expanding number of endpoints in your data centre or virtualised environments led to any security breaches?



Strategy in place: Keeping data safe when moving across application and endpoints	Response (%)
Yes	55.7%
No	44.3%

What is the priority level of each of these corporate initiatives in your organisation?

High priority of corporate initiatives (5 only)

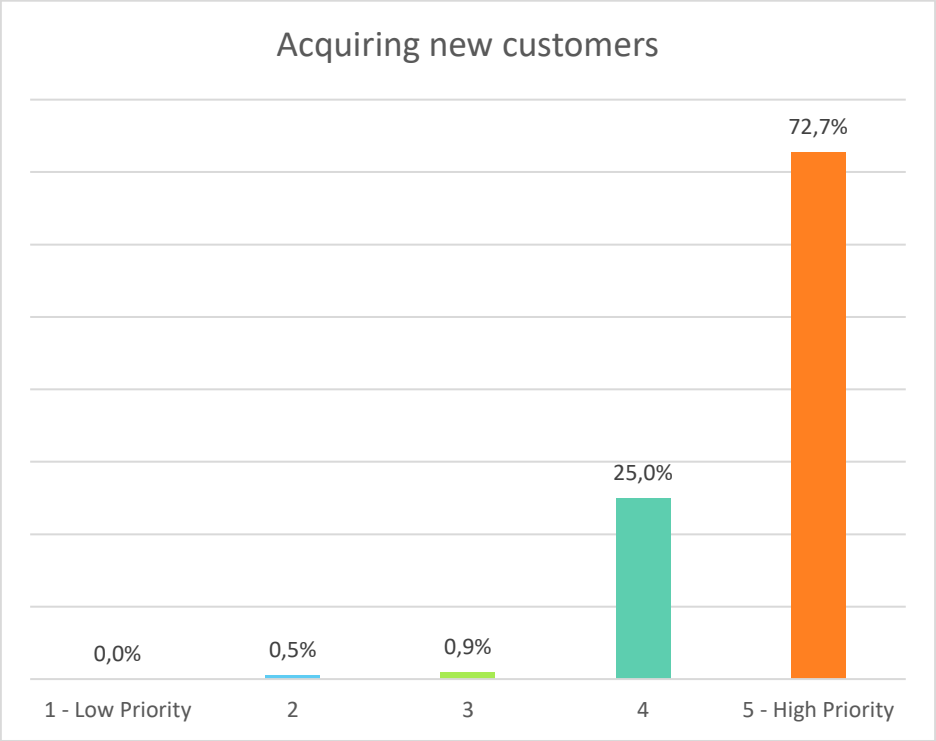


High priority of corporate initiative	**Response (%)**
Acquiring new customers	72.7%
Growing existing customers revenue	71.8%
Ensuring regulatory compliance	60.0%
Reducing costs	58.6%
Protecting against cyber Attacks	58.6%
Growing internationally	58.6%
Launching new products and services	57.7%
Data security	56.8%
Fostering innovation and creativity	55.0%

Overall priority of corporate initiatives (4/5 combined)

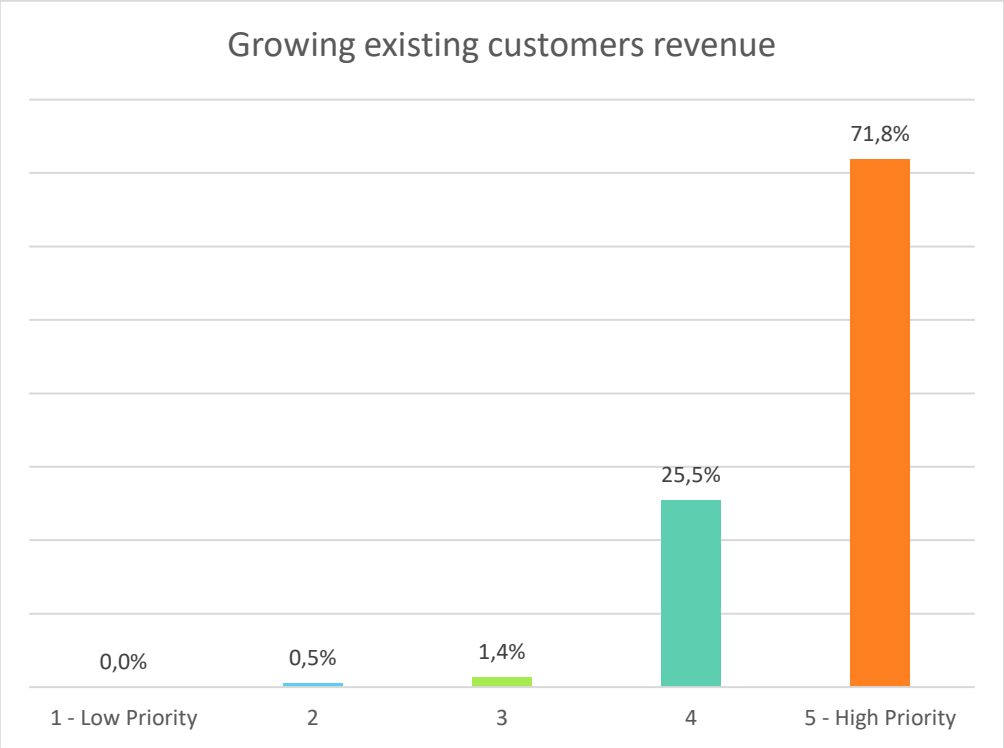
Overall priority of corporate initiative	**Response (%)**
Acquiring new customers	97.7%
Growing existing customers revenue	97.3%
Reducing costs	85.5%
Ensuring regulatory compliance	84.5%
Protecting against cyber Attacks	86.8%
Growing internationally	81.4%
Fostering innovation and creativity	81.4%
Launching new products and services	82.3%
Data security	81.4%

Acquiring new customers



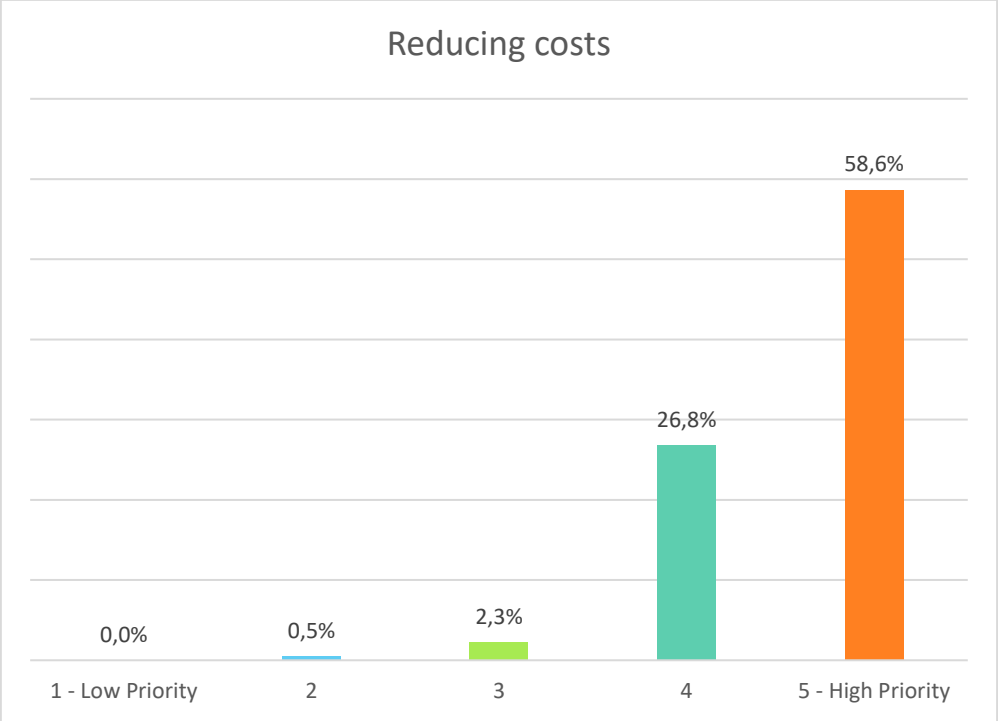
Acquiring new customers	Response (%)
1 - Low Priority	0.0%
2	0.5%
3	0.9%
4	25.0%
5 - High Priority	72.7%

Growing existing customers revenue



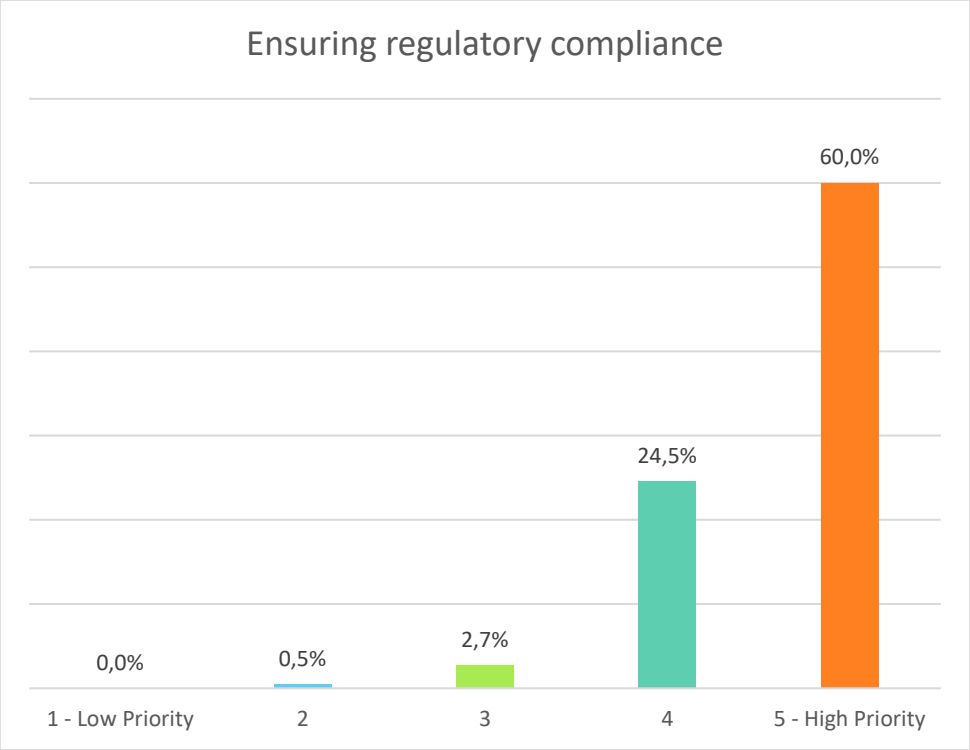
Growing existing customers revenue	Response (%)
1 - Low Priority	0.0%
2	0.5%
3	1.4%
4	25.5%
5 - High Priority	71.8%

Reducing costs



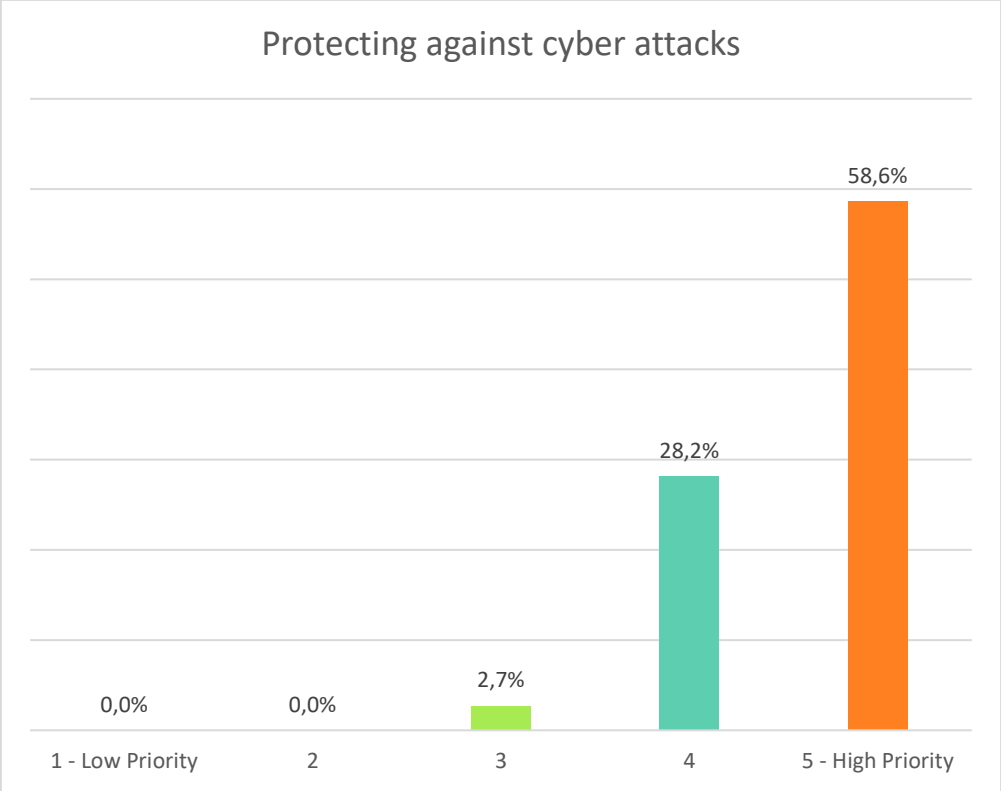
Reducing costs	Response (%)
1 - Low Priority	0.0%
2	0.5%
3	2.3%
4	26.8%
5 - High Priority	58.6%

Ensuring regulatory compliance



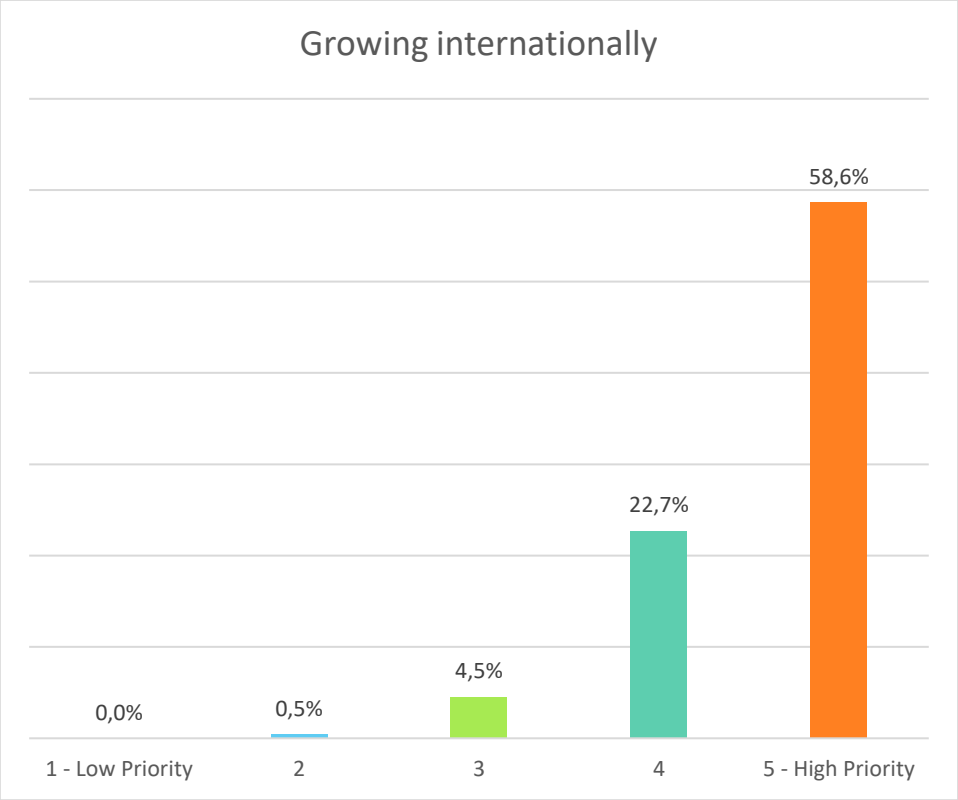
Ensuring regulatory compliance	Response (%)
1 - Low Priority	0.0%
2	0.5%
3	2.7%
4	24.5%
5 - High Priority	60.0%

Protecting against cyber attacks



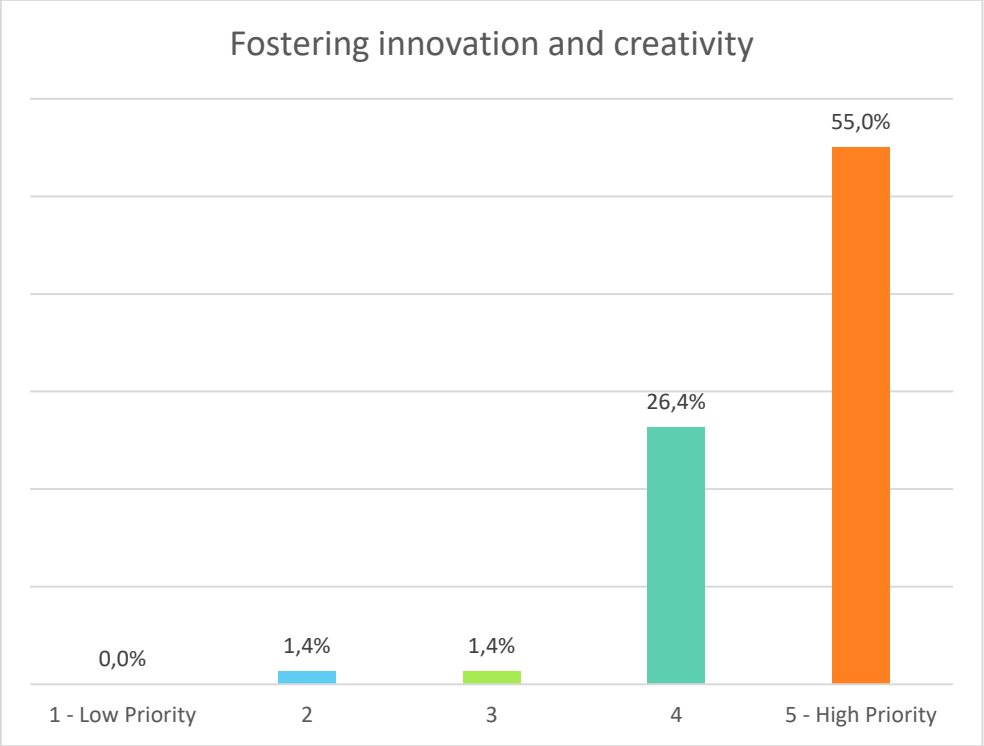
Protecting against cyber attacks	Response (%)
1 - Low Priority	0.0%
2	0.0%
3	2.7%
4	28.2%
5 - High Priority	58.6%

Growing internationally



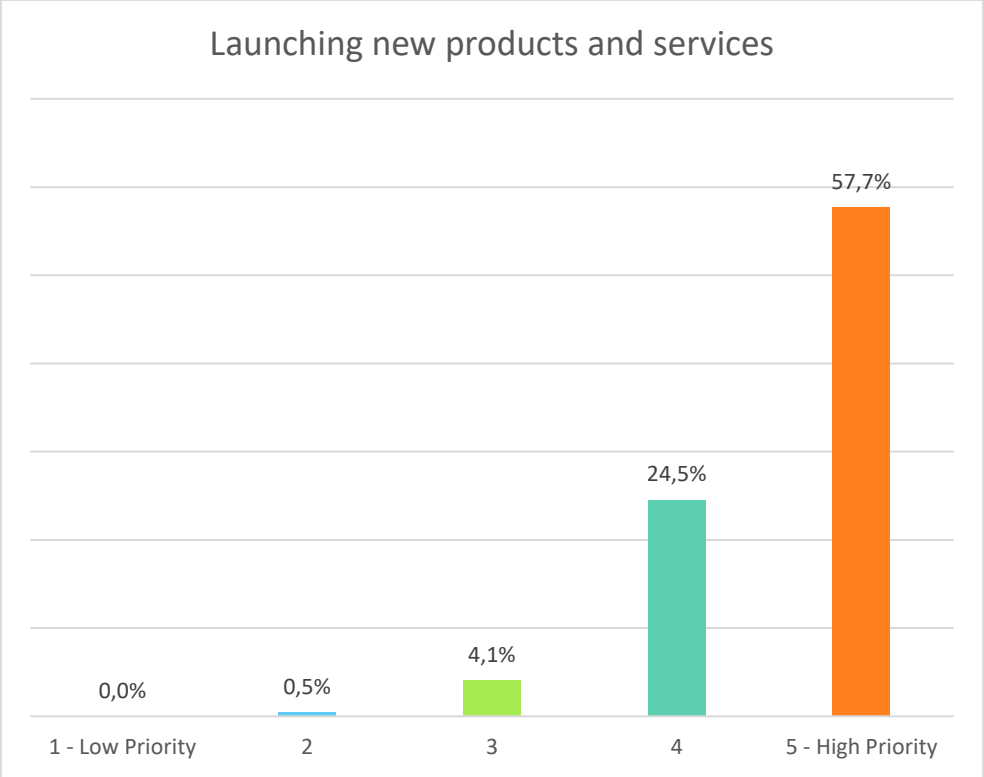
Growing internationally	Response (%)
1 - Low Priority	0.0%
2	0.5%
3	4.5%
4	22.7%
5 - High Priority	58.6%

Fostering innovation and creativity



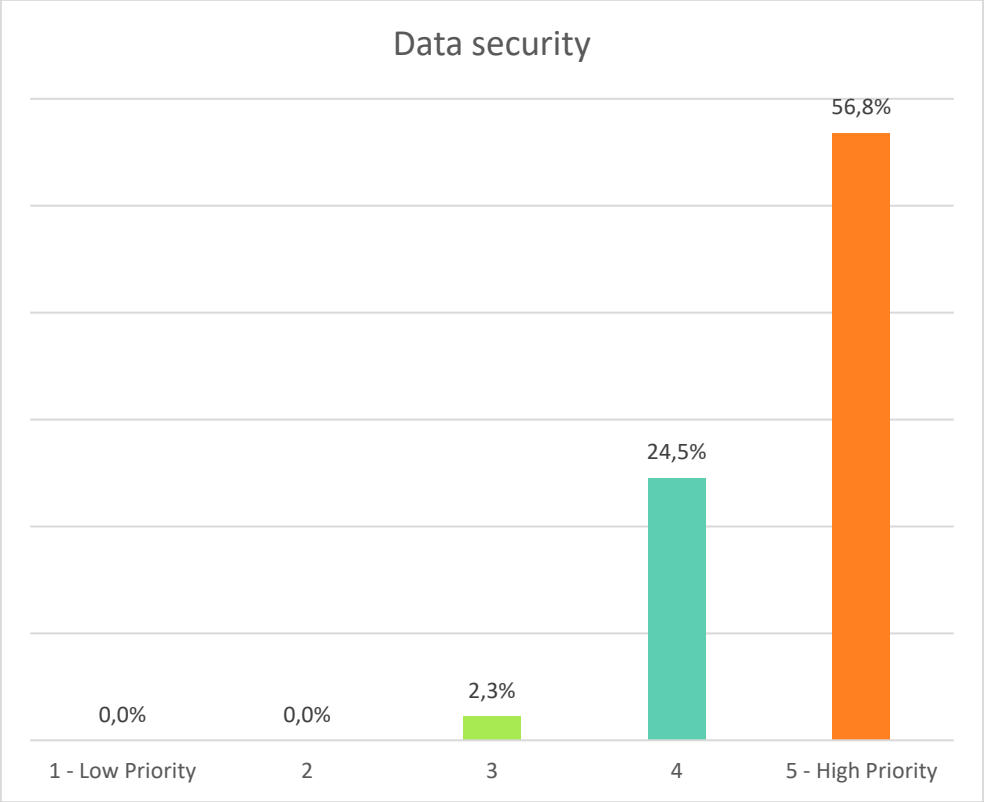
Fostering innovation and creativity	Response (%)
1 - Low Priority	0.0%
2	1.4%
3	1.4%
4	26.4%
5 - High Priority	55.0%

Launching new products and services



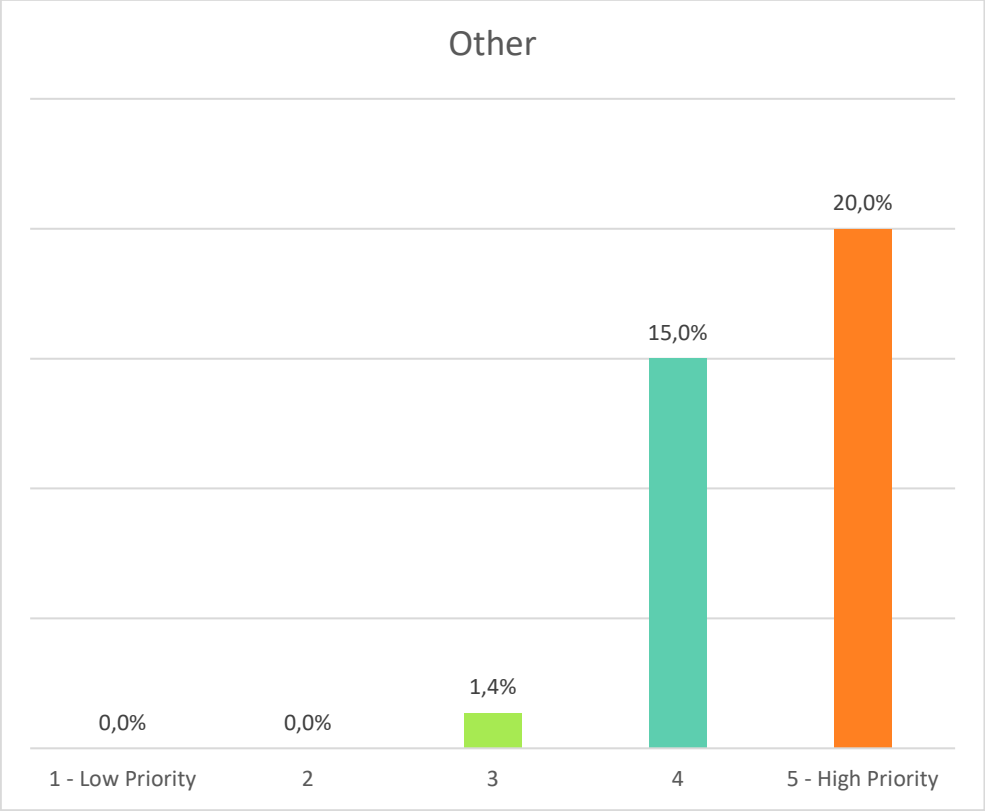
Launching new products and services	Response (%)
1 - Low Priority	0.0%
2	0.5%
3	4.1%
4	24.5%
5 - High Priority	57.7%

Data security



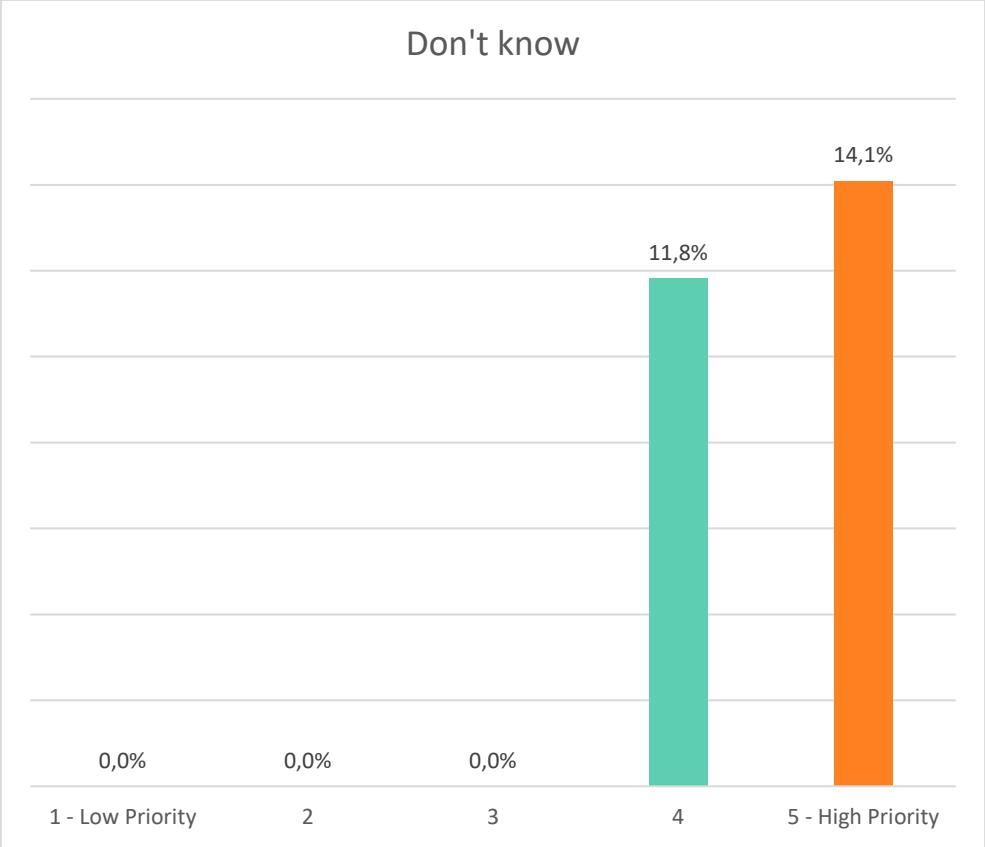
Data security	Response (%)
1 - Low Priority	0.0%
2	0.0%
3	2.3%
4	24.5%
5 - High Priority	56.8%

Other



Other	Response (%)
1 - Low Priority	0.0%
2	0.0%
3	1.4%
4	15.0%
5 - High Priority	20.0%

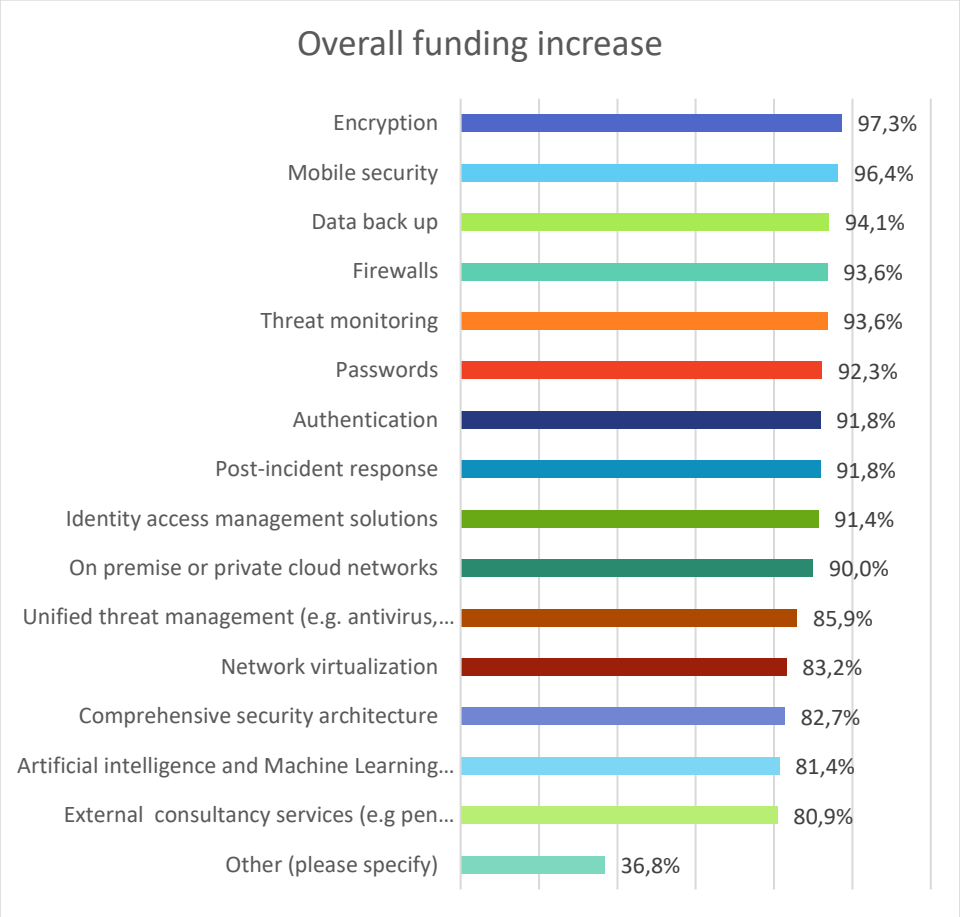
Don't know



Don’t know	Response (%)
1 - Low Priority	0.0%
2	0.0%
3	0.0%
4	11.8%
5 - High Priority	14.1%

Funding change for the following cyber security solutions in the next five years

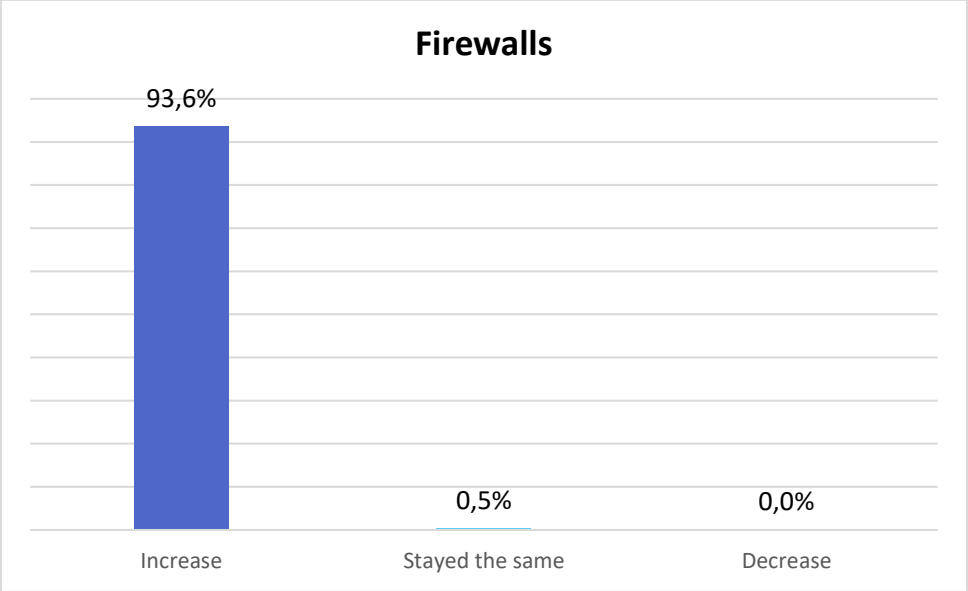
Overall funding increase



Overall increase	**Response (%)**
Encryption	97.3%
Mobile security	96.4%
Data back up	94.1%
Firewalls	93.6%
Threat monitoring	93.6%
Passwords	92.3%
Authentication	91.8%
Post-incident response	91.8%
Identity access management solutions	91.4%
On premise or private cloud networks	90.0%
Unified threat management (e.g. antivirus, malware, URL filtering etc)	85.9%
Network virtualization	83.2%
Comprehensive security architecture	82.7%
Artificial intelligence and Machine Learning for automated security	81.4%

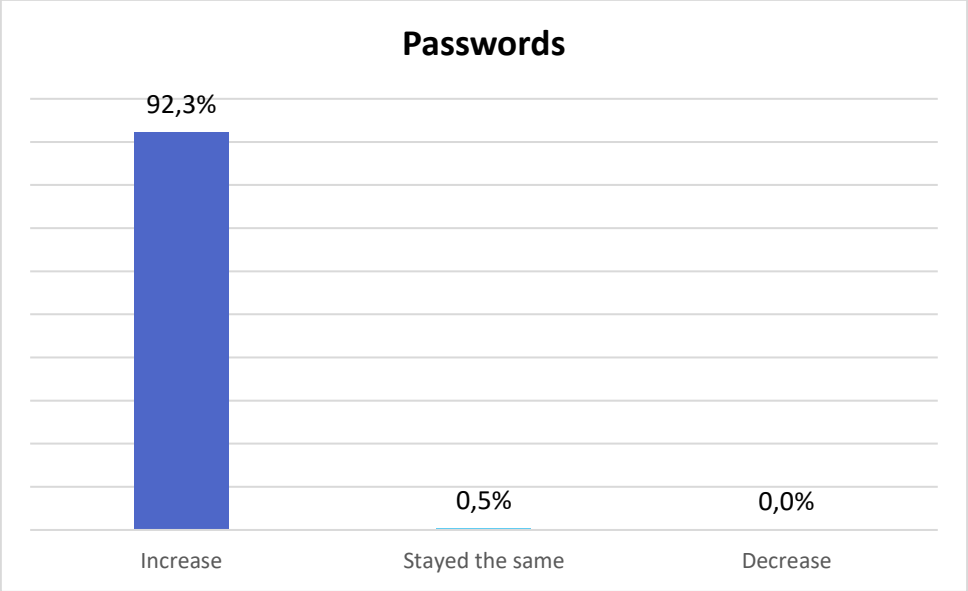
External consultancy services (e.g. pen testing, security audits etc.)	80.9%
Other (please specify)	36.8%

Firewalls



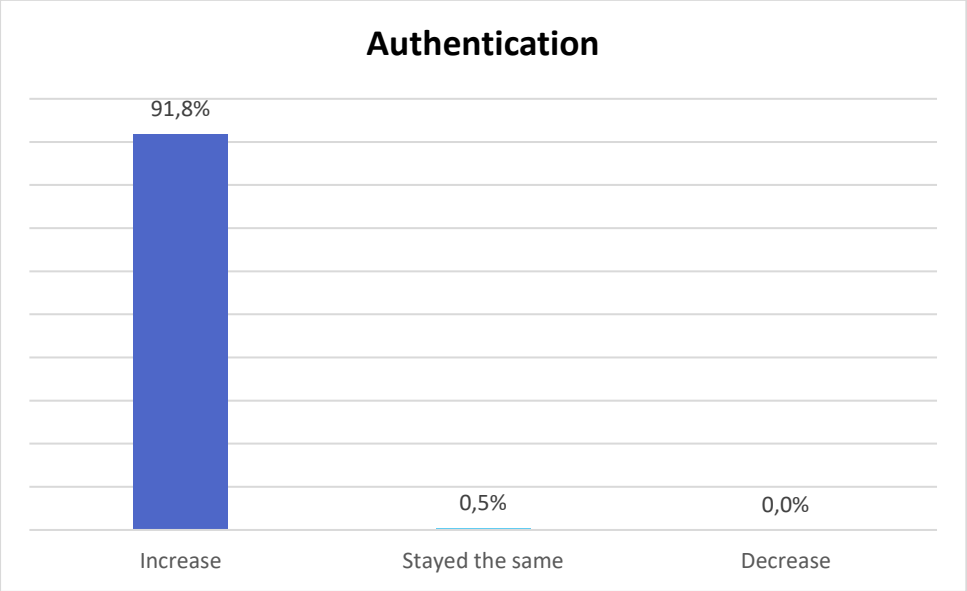
Firewalls	Response (%)
Increase	93.6%
Stayed the same	0.5%
Decrease	0.0%

Passwords



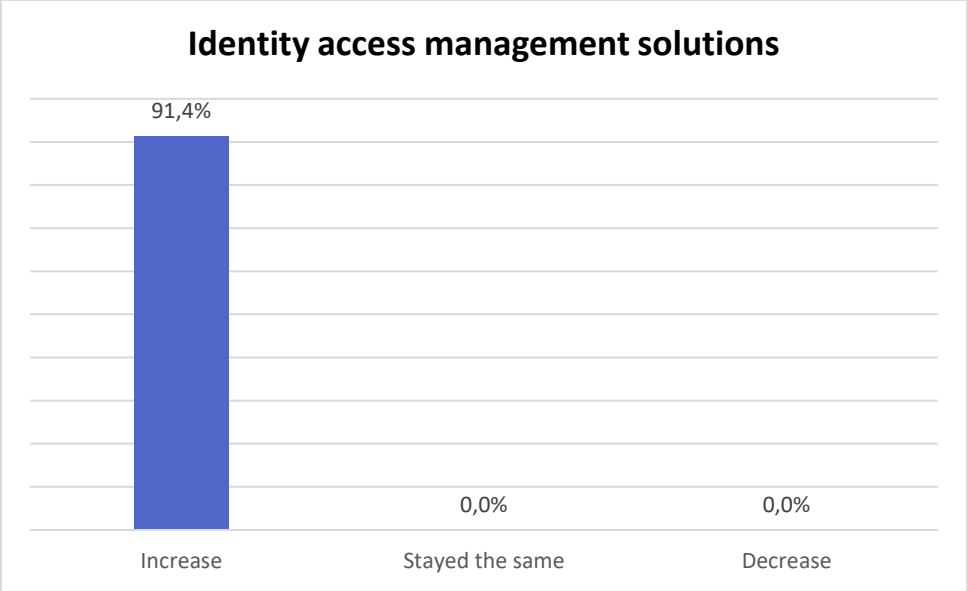
Passwords	Response (%)
Increase	92.3%
Stayed the same	0.5%
Decrease	0.0%

Authentication



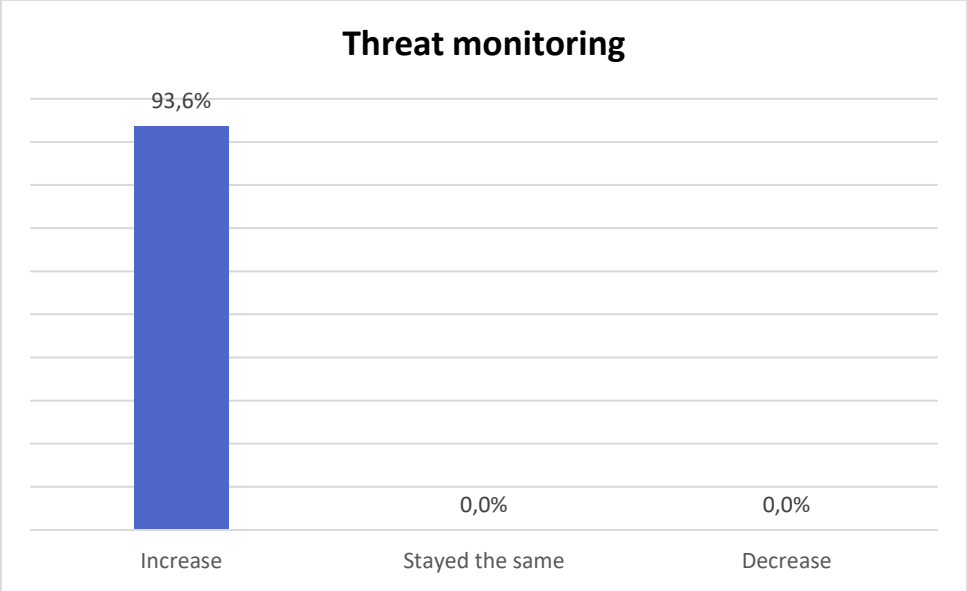
Authentication	Response (%)
Increase	91.8%
Stayed the same	0.5%
Decrease	0.0%

Identity access management solutions



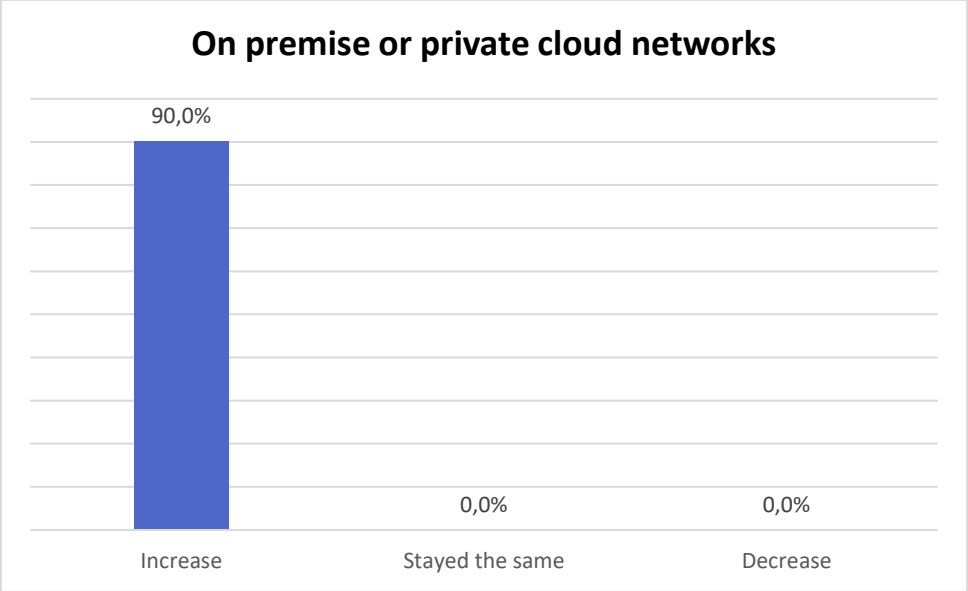
Identity access management solutions	Response (%)
Increase	91.4%
Stayed the same	0.0%
Decrease	0.0%

Threat monitoring



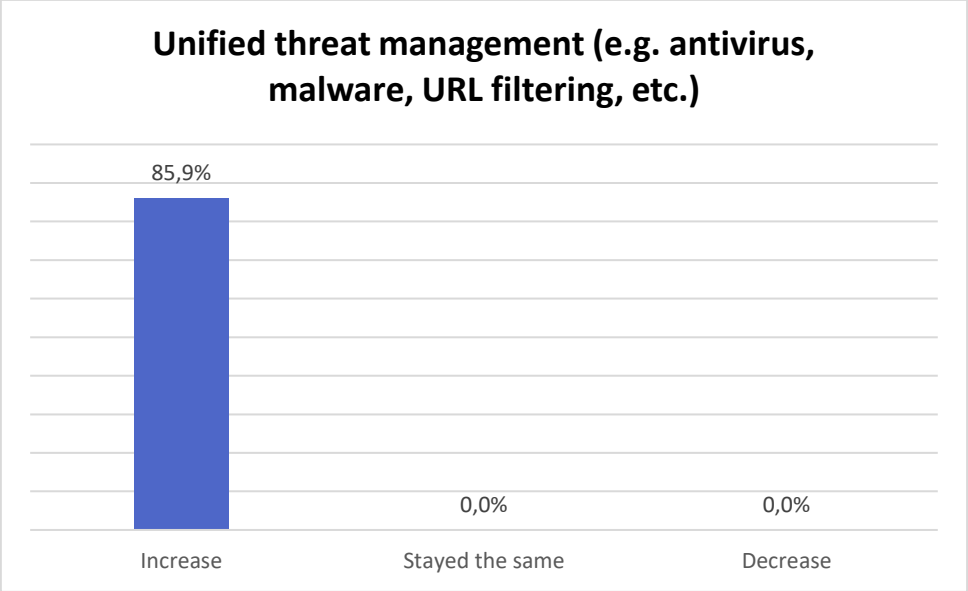
Threat monitoring	Response (%)
Increase	93.6%
Stayed the same	0.0%
Decrease	0.0%

On premise or private cloud networks



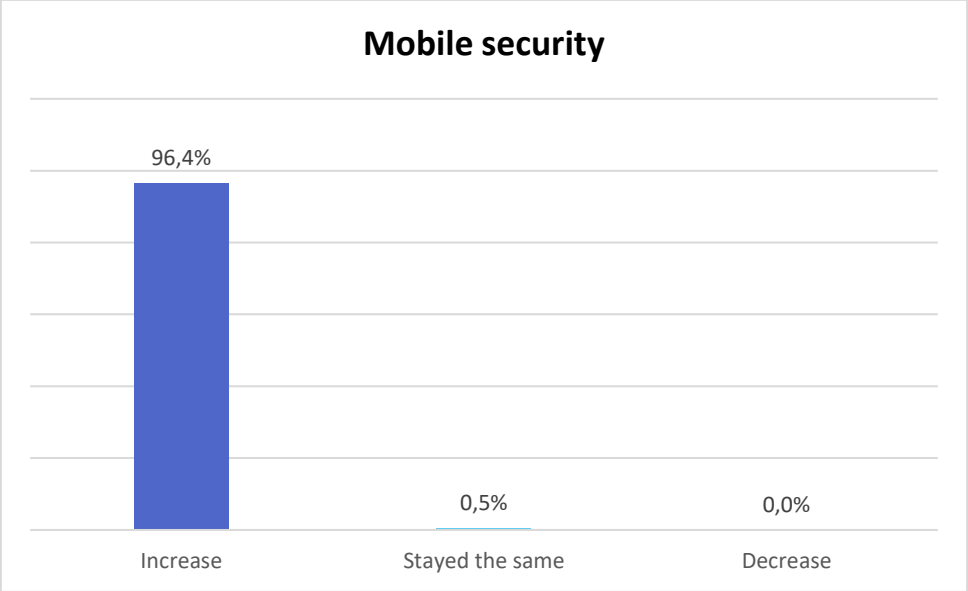
On premise or private cloud networks	Response (%)
Increase	90.0%
Stayed the same	0.0%
Decrease	0.0%

Unified threat management (e.g. antivirus, malware, URL filtering, etc.)



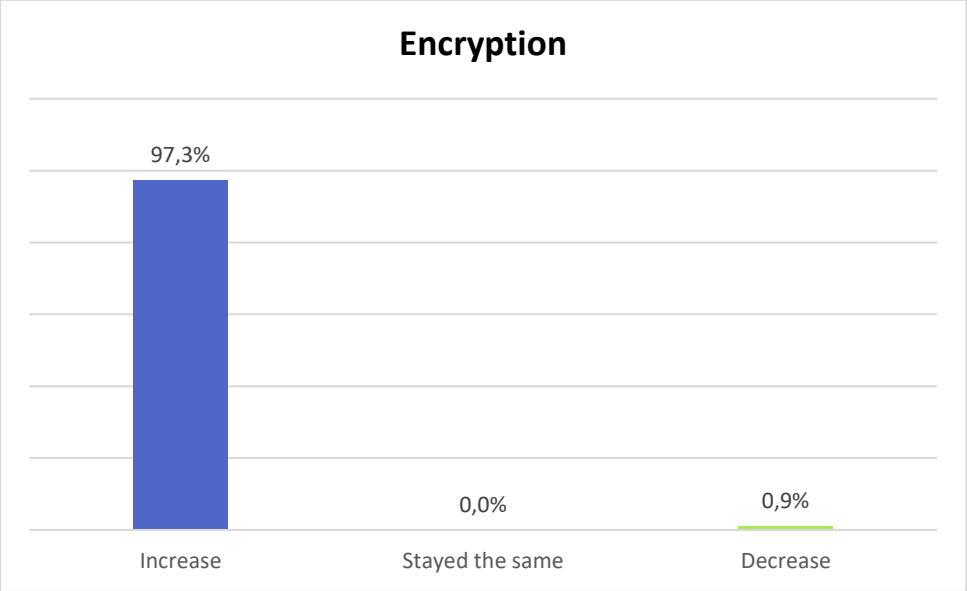
Unified threat management	Response (%)
Increase	85.9%
Stayed the same	0.0%
Decrease	0.0%

Mobile security



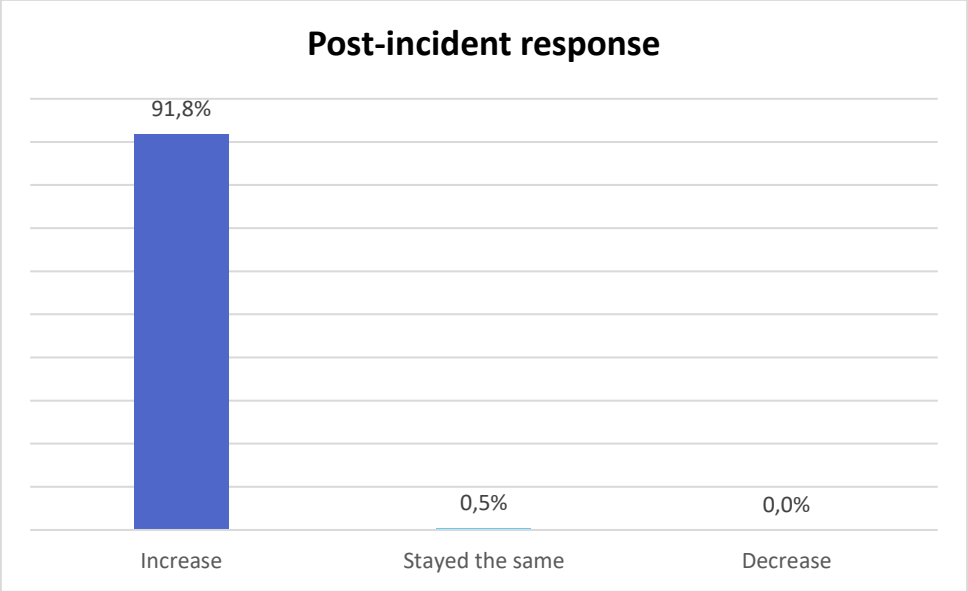
Mobile security	Response (%)
Increase	96.4%
Stayed the same	0.5%
Decrease	0.0%

Encryption



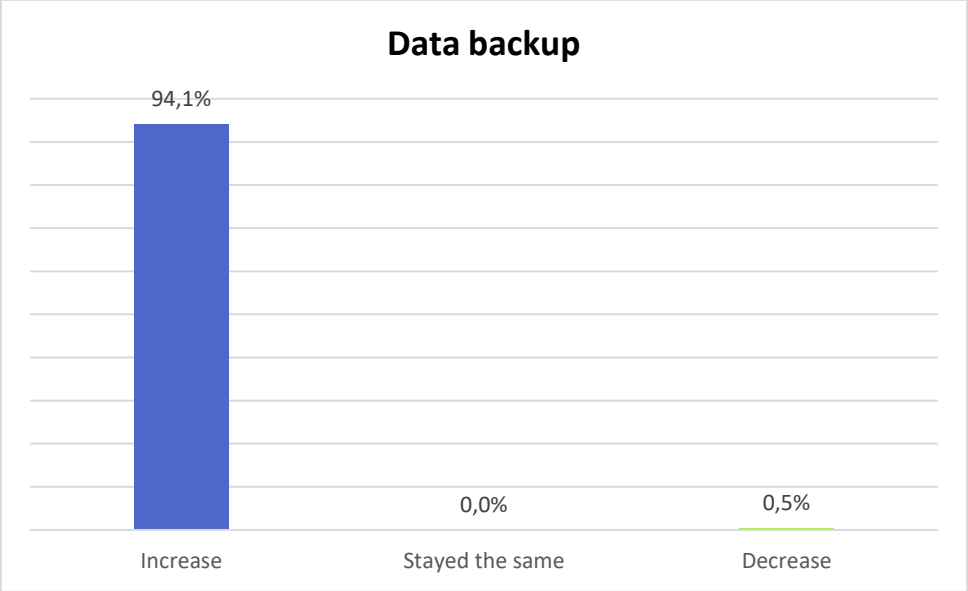
Encryption	Response (%)
Increase	97.3%
Stayed the same	0.0%
Decrease	0.9%

Post-incident response



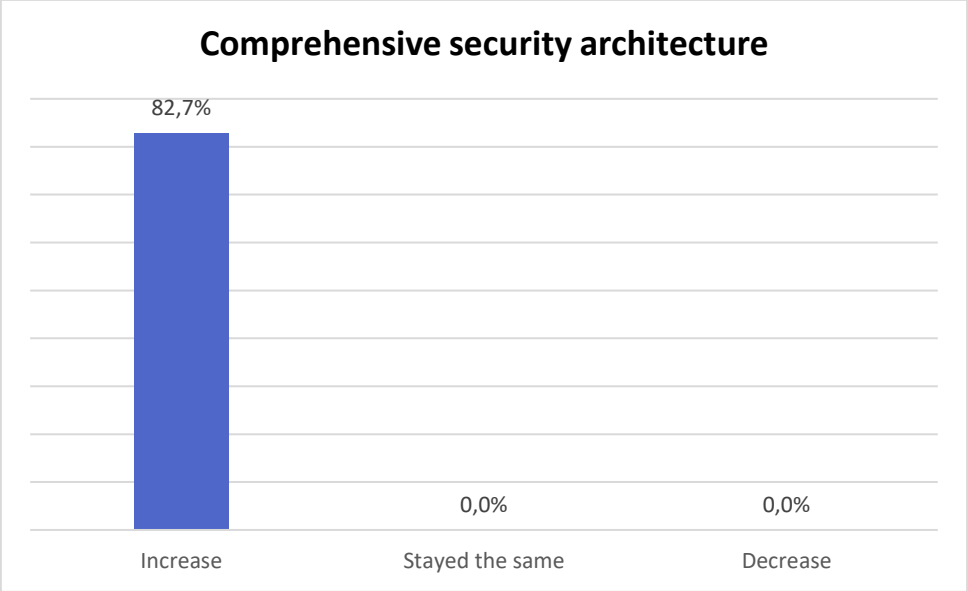
Post-incident response	Response (%)
Increase	91.8%
Stayed the same	0.5%
Decrease	0.0%

Data backup



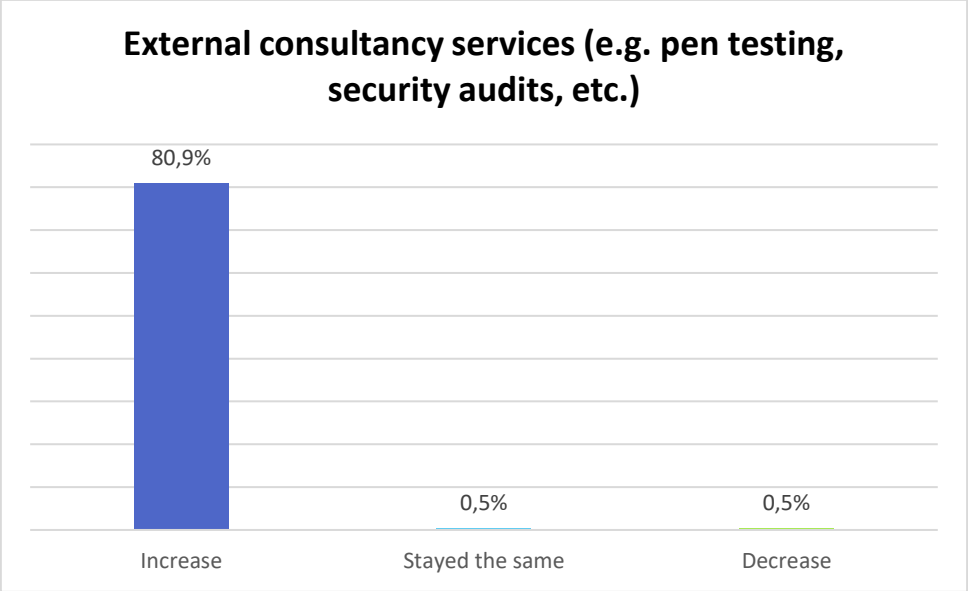
Data backup	Response (%)
Increase	94.1%
Stayed the same	0.0%
Decrease	0.5%

Comprehensive security architecture



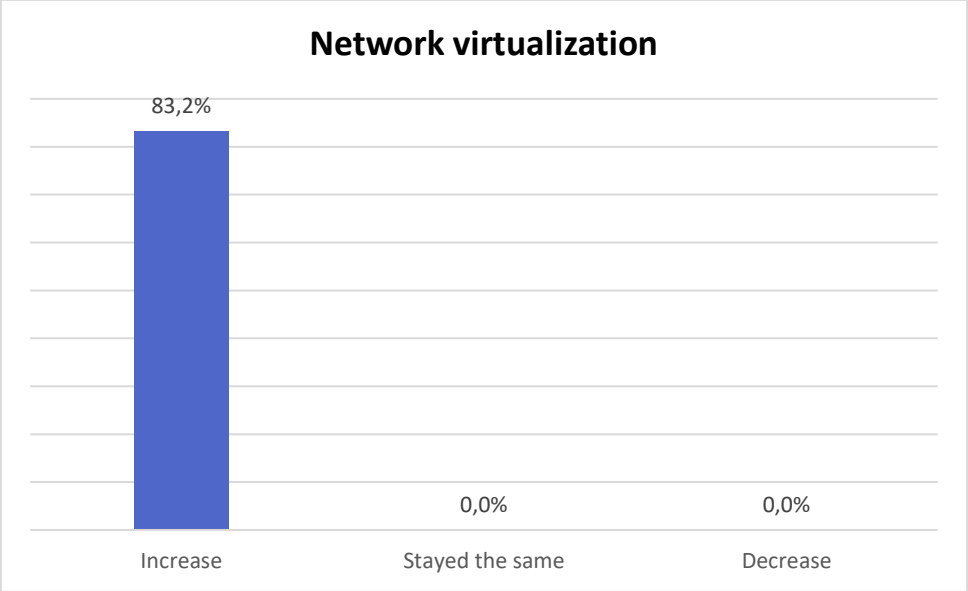
Comprehensive security architecture	Response (%)
Increase	82.7%
Stayed the same	0.0%
Decrease	0.0%

External consultancy services (e.g. pen testing, security audits, etc.)



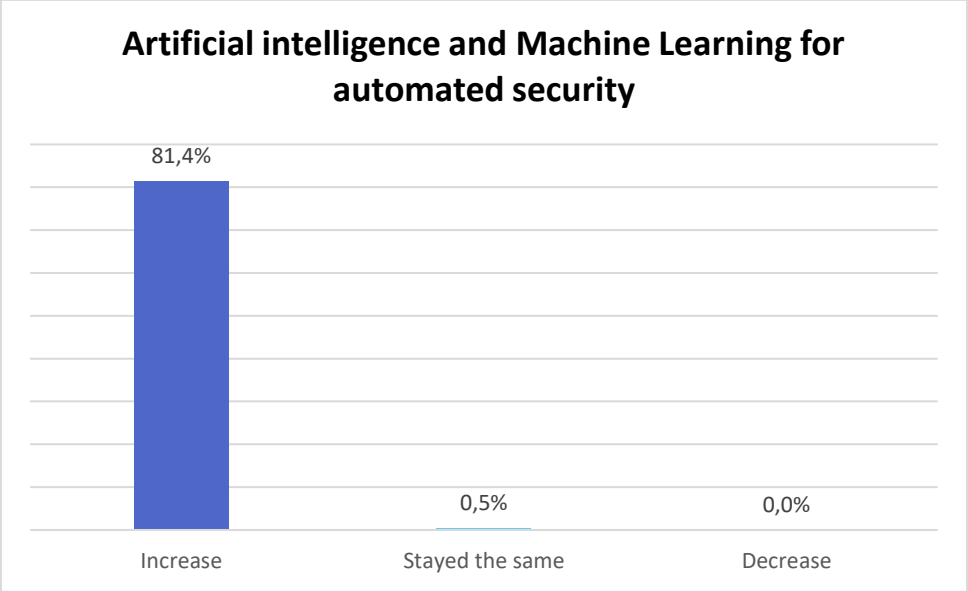
External consultancy services	Response (%)
Increase	80.9%
Stayed the same	0.5%
Decrease	0.5%

Network virtualization



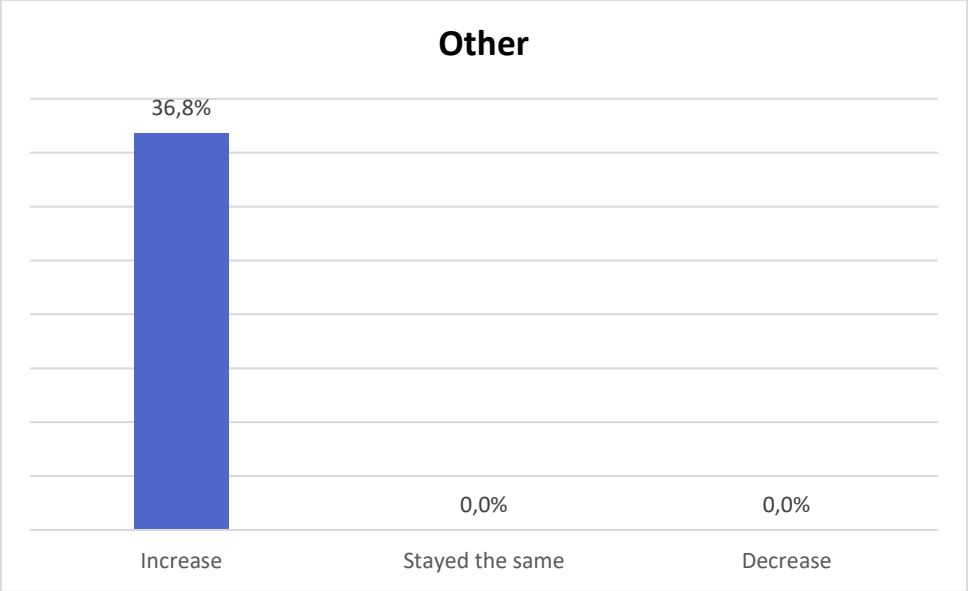
Network virtualization	Response (%)
Increase	83.2%
Stayed the same	0.0%
Decrease	0.0%

Artificial intelligence and Machine Learning for automated security



AI and ML for automated security	Response (%)
Increase	81.4%
Stayed the same	0.5%
Decrease	0.0%

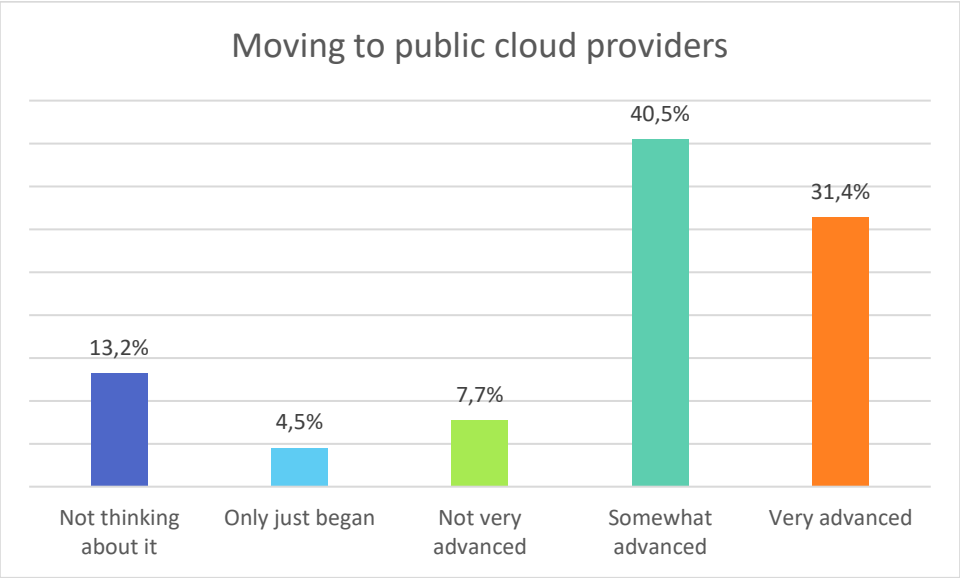
Other



Other	Response (%)
Increase	36.8%
Stayed the same	0.0%
Decrease	0.0%

Moving applications and storage to major cloud providers

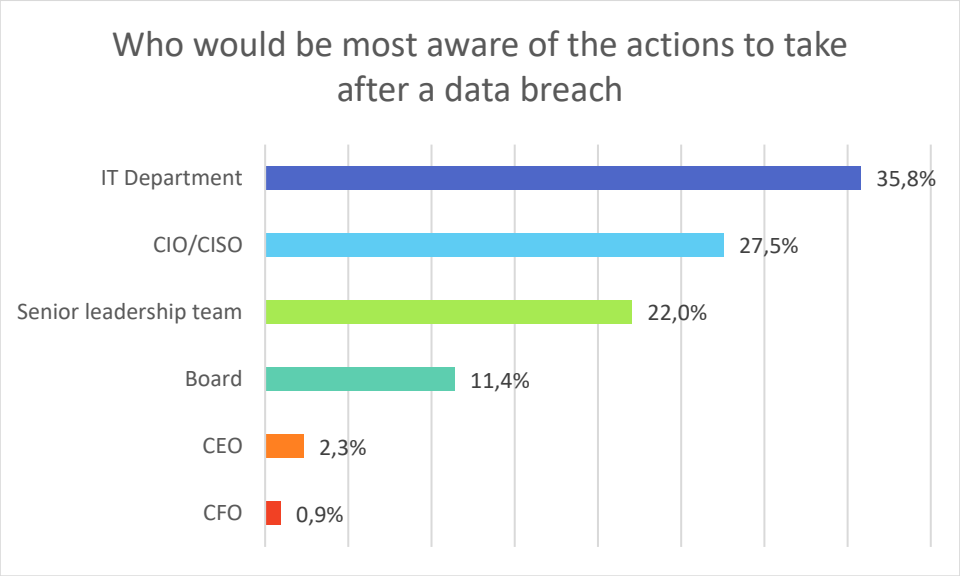
How far advanced is your organisation in moving applications and storage to major cloud providers like AWS, Microsoft Azure and Google Cloud?



Moving to public cloud providers	Response (%)
Not thinking about it	13.2%
Only just began	4.5%
Not very advanced	7.7%
Somewhat advanced	40.5%
Very advanced	31.4%

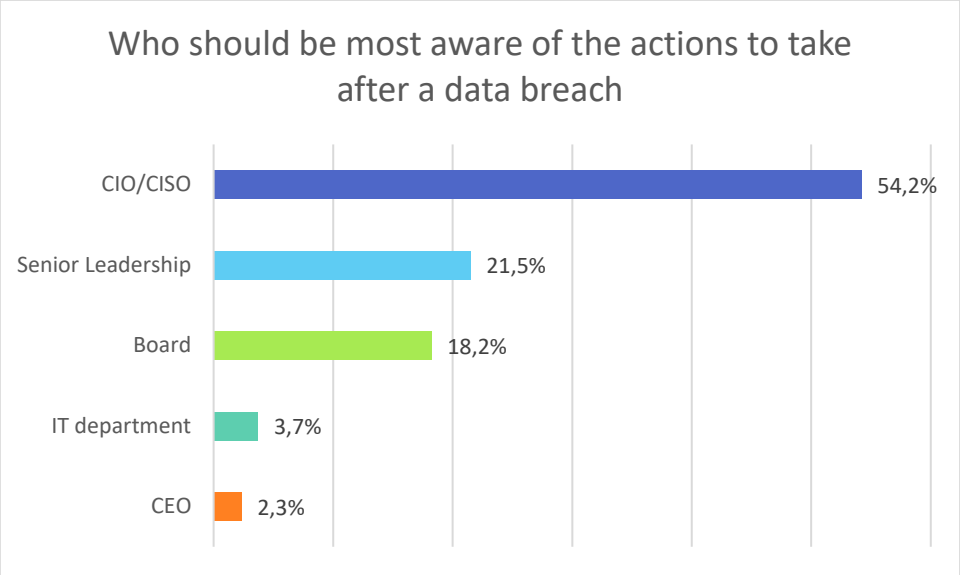
Security and Vulnerability

Who would be most aware of the actions to take after a data breach?



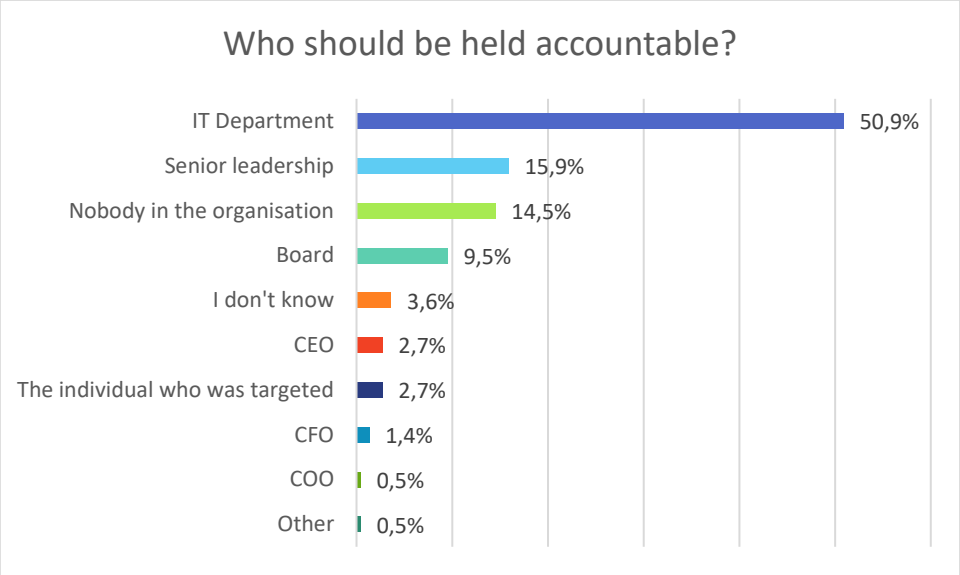
Who would be most aware of the actions to take after a data breach?	Responses (%)
IT Department	35.8%
CIO/CISO	27.5%
Senior leadership team	22.0%
Board	11.4%
CEO	2.3%
CFO	0.9%

Who should be most aware of the actions to take after a data breach?



Who should be most aware of the actions to take after a data breach?	Response (%)
CIO/CISO	54.2%
Senior Leadership	21.5%
Board	18.2%
IT department	3.7%
CEO	2.3%

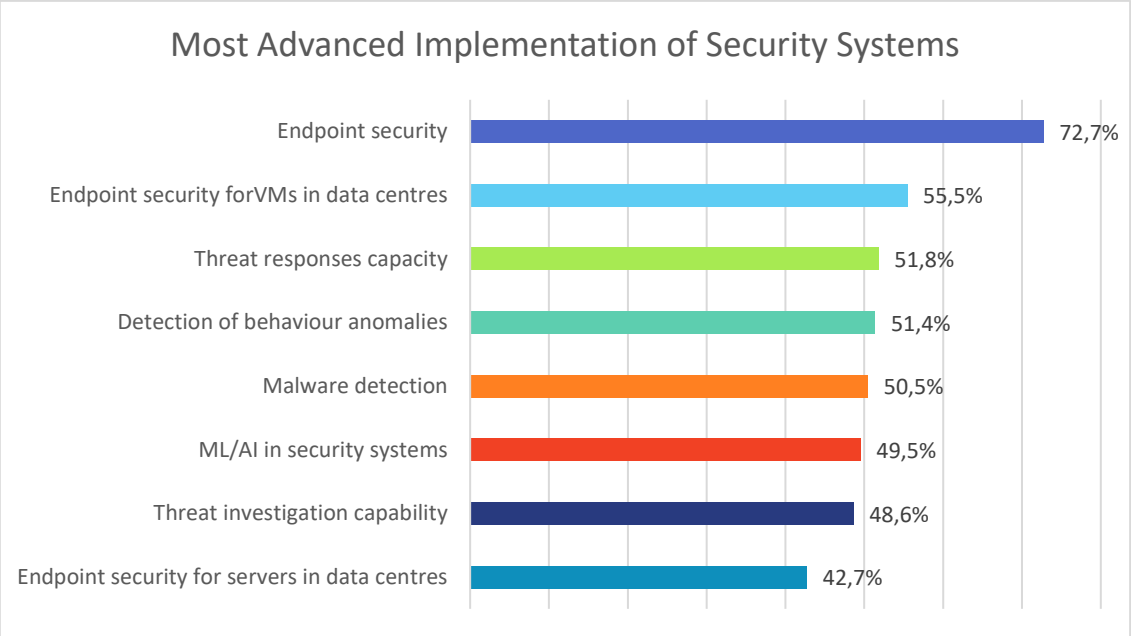
Who should be held accountable for a data or security breach?



Who should be held accountable?	Responses (%)
IT Department	50.9%
Senior leadership	15.9%
Nobody in the organisation	14.5%
Board	9.5%
I don't know	3.6%
CEO	2.7%
The individual who was targeted	2.7%
CFO	1.4%
COO	0.5%
Other	0.5%

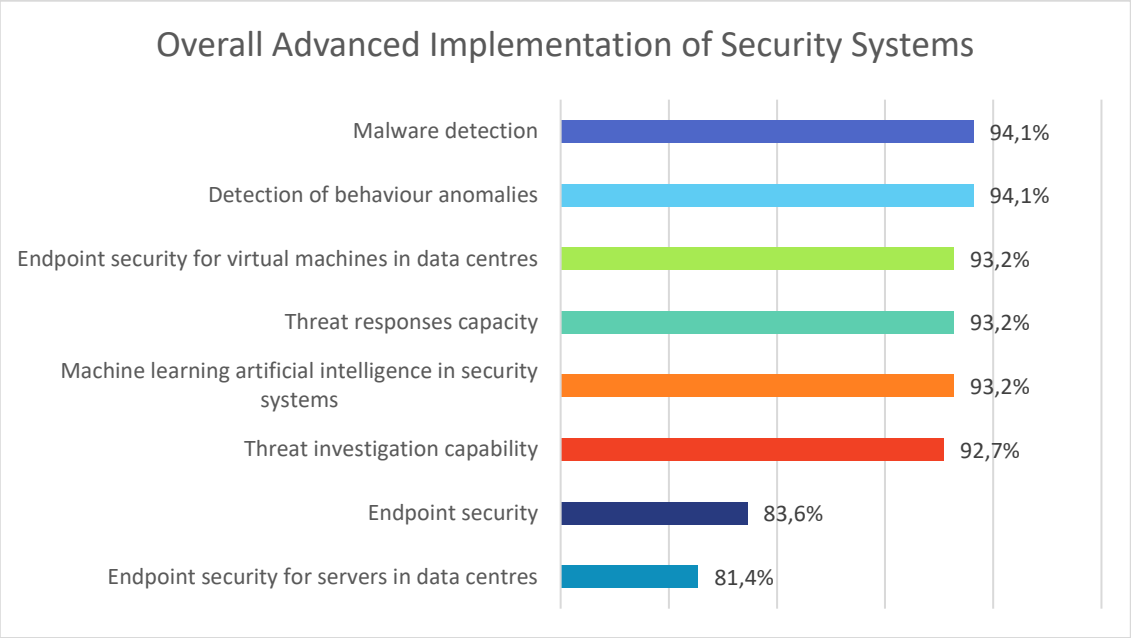
How advanced are you in implementing each of these security solutions in your organisation?

Most advanced only (5 only)



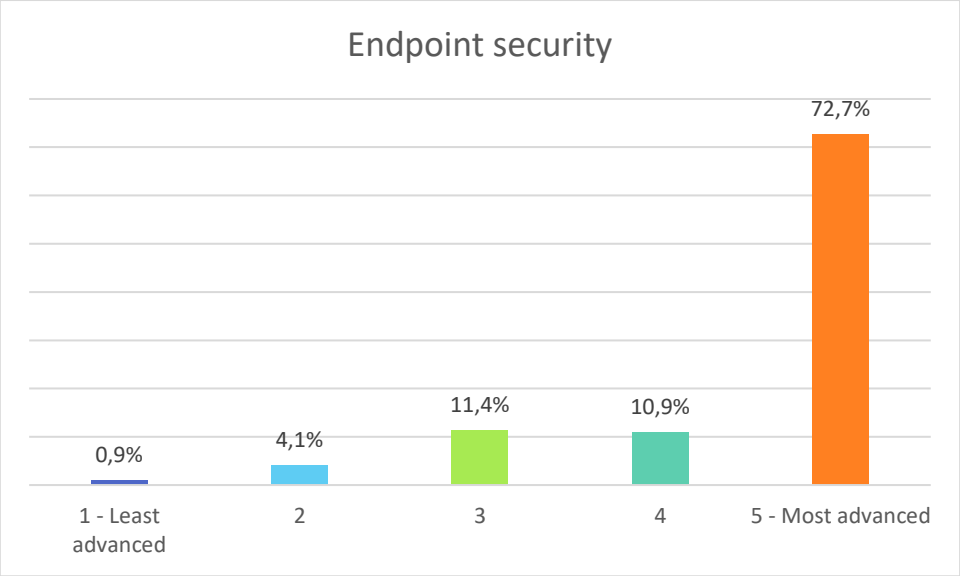
Most advanced implementation	Response (%)
Endpoint security	72.7%
Endpoint security for VMs in data centres	55.5%
Threat responses capacity	51.8%
Detection of behaviour anomalies	51.4%
Malware detection	50.5%
ML/AI in security systems	49.5%
Threat investigation capability	48.6%
Endpoint security for servers in data centres	42.7%

Overall advanced (4/5 combined)



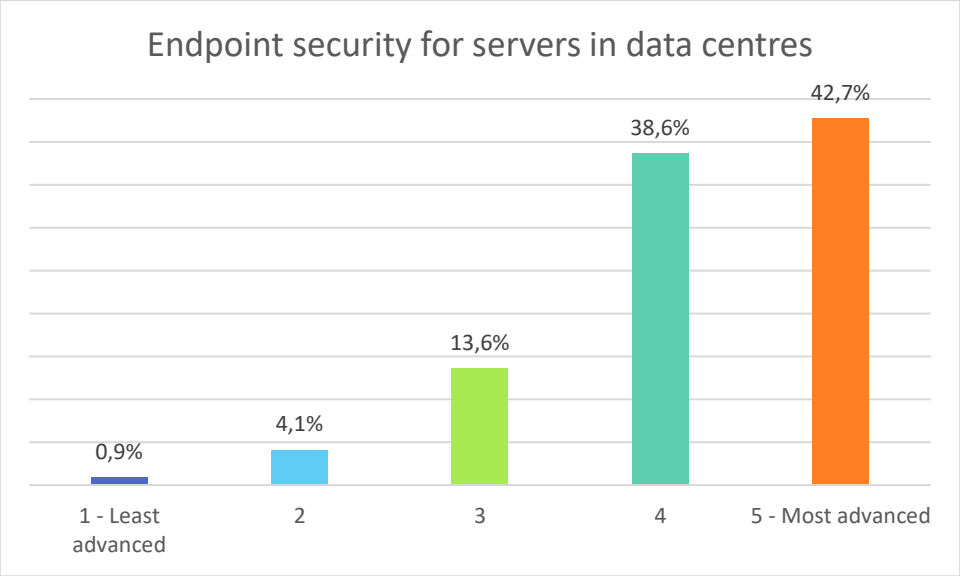
Overall advanced implementation	**Response (%)**
Malware detection	94.1%
Detection of behaviour anomalies	94.1%
Endpoint security for virtual machines in data centres	93.2%
Threat responses capacity	93.2%
Machine learning artificial intelligence in security systems	93.2%
Threat investigation capability	92.7%
Endpoint security	83.6%
Endpoint security for servers in data centres	81.4%

Endpoint security



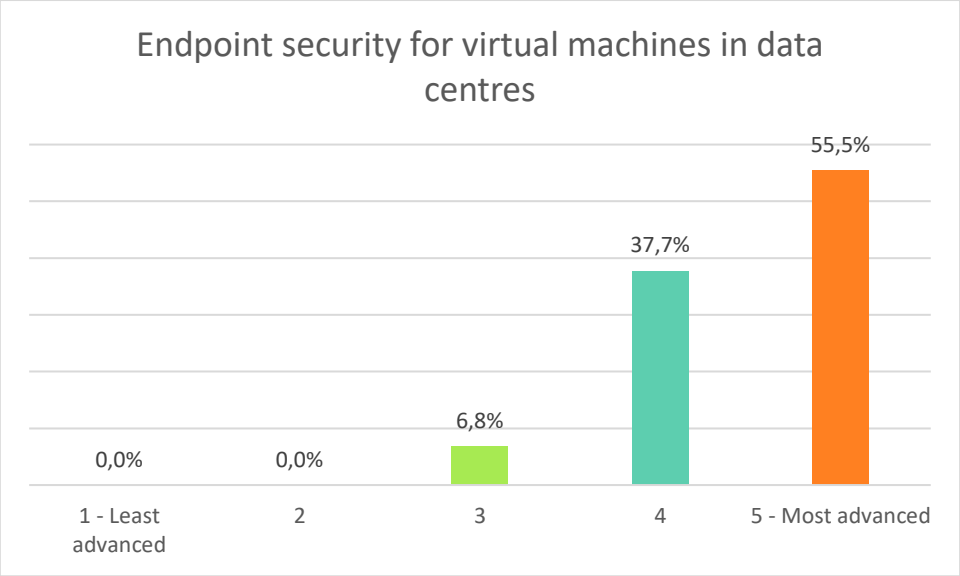
Endpoint security	Response (%)
1 - Least advanced	0.9%
2	4.1%
3	11.4%
4	10.9%
5 - Most advanced	72.7%

Endpoint security for servers in data centres



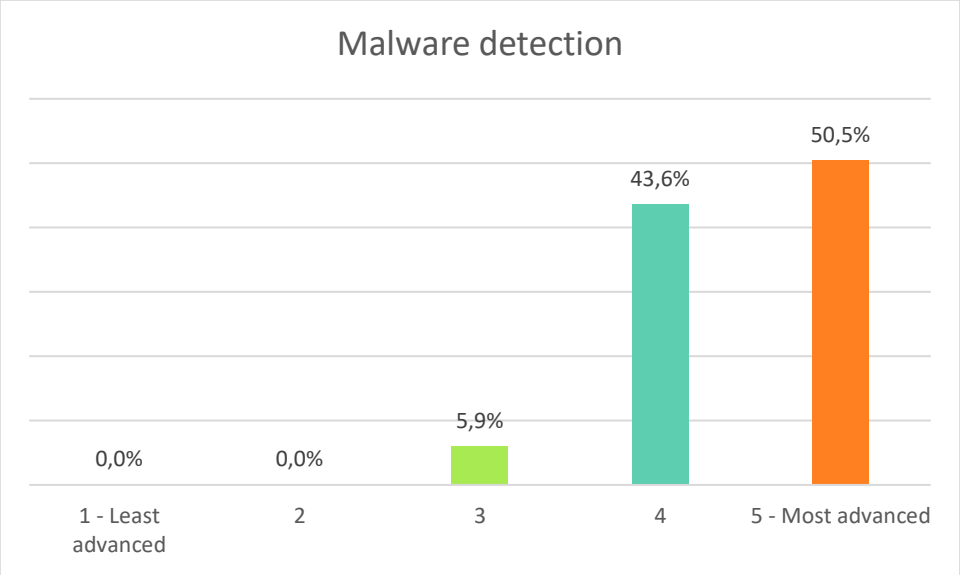
Endpoint security for servers in data centres	Response (%)
1 - Least advanced	0.9%
2	4.1%
3	13.6%
4	38.6%
5 - Most advanced	42.7%

Endpoint security for virtual machines in data centres



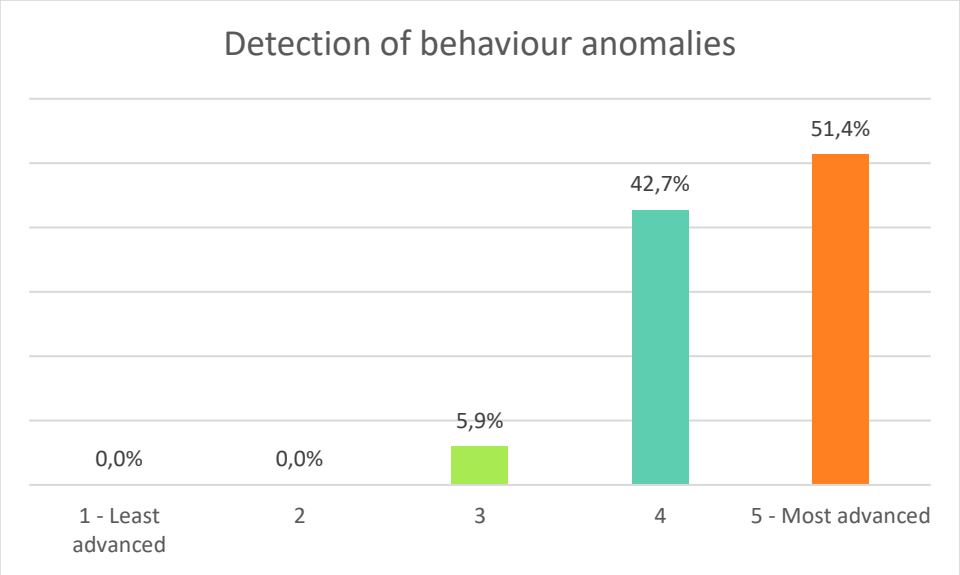
Endpoint security for virtual machines	Response (%)
1 - Least advanced	0.0%
2	0.0%
3	6.8%
4	37.7%
5 - Most advanced	55.5%

Malware detection



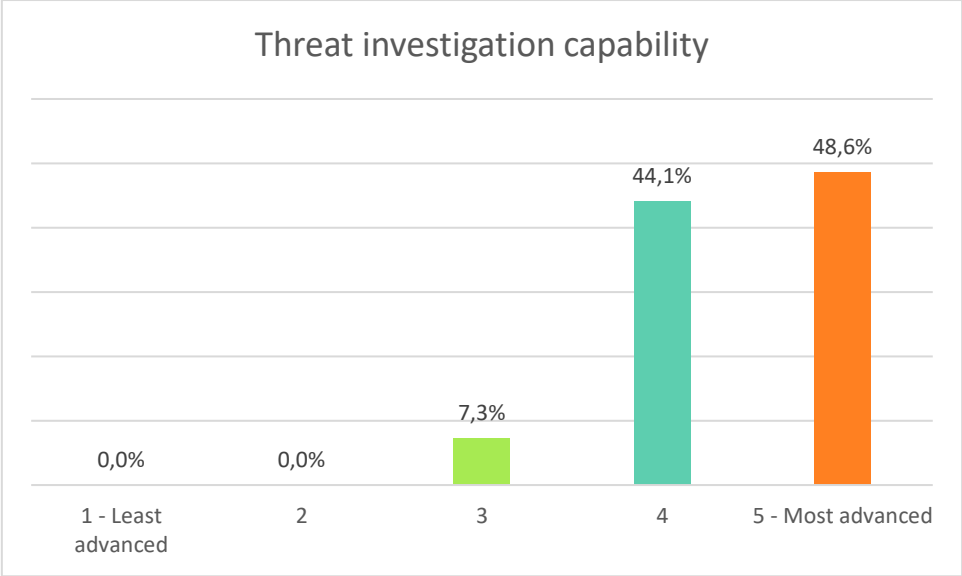
Malware detection	Response (%)
1 - Least advanced	0.0%
2	0.0%
3	5.9%
4	43.6%
5 - Most advanced	50.5%

Detection of behaviour anomalies



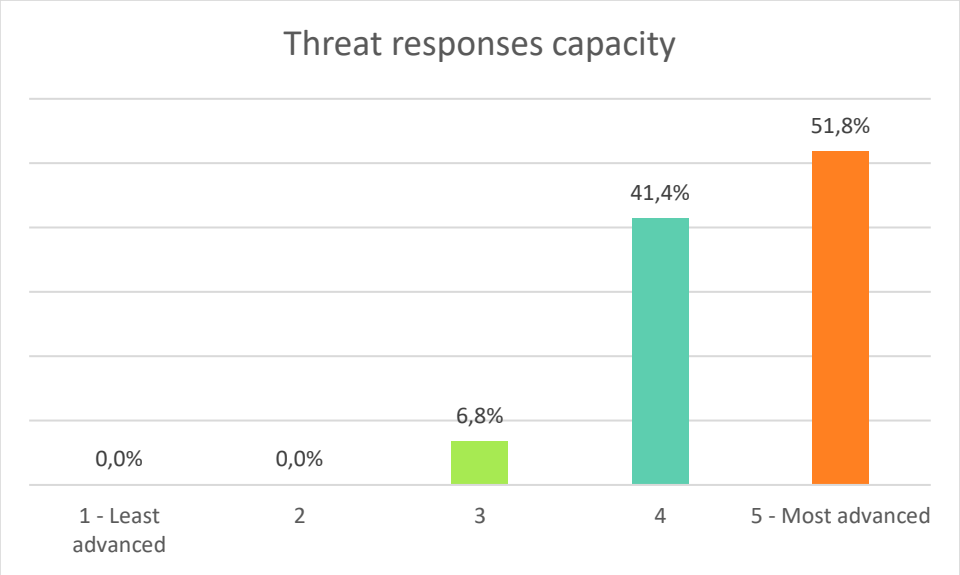
Detection of behaviour anomalies	Response (%)
1 - Least advanced	0.0%
2	0.0%
3	5.9%
4	42.7%
5 - Most advanced	51.4%

Threat investigation capability



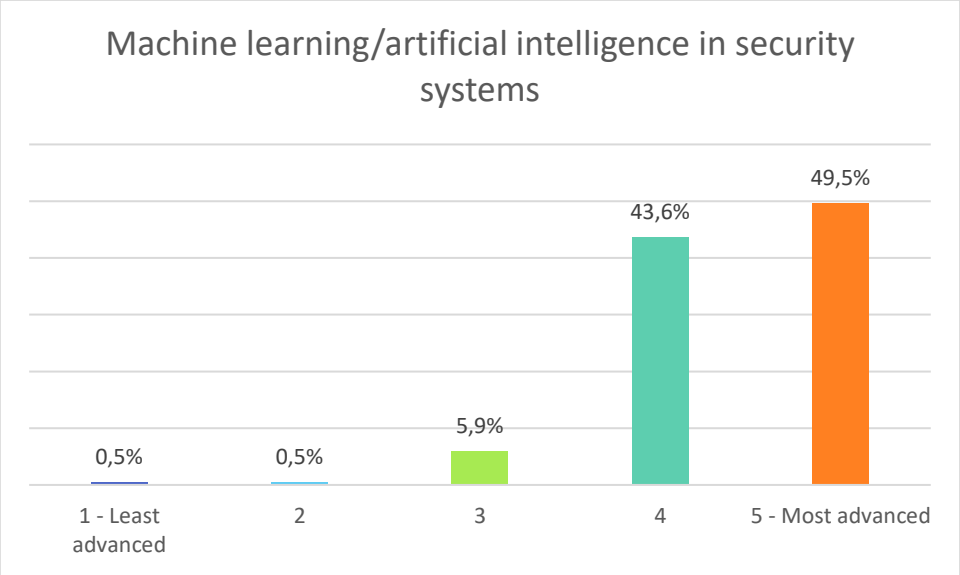
Threat investigation capability	Response (%)
1 - Least advanced	0.0%
2	0.0%
3	7.3%
4	44.1%
5 - Most advanced	48.6%

Threat responses capacity



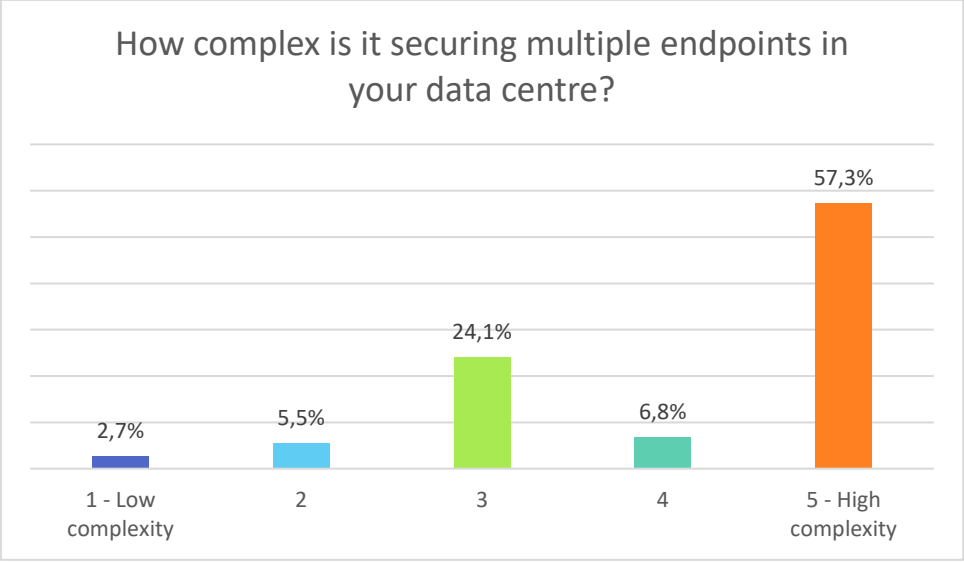
Threat responses capability	Response (%)
1 - Least advanced	0.0%
2	0.0%
3	6.8%
4	41.4%
5 - Most advanced	51.8%

Machine learning/artificial intelligence in security systems



Machine learning/artificial intelligence in security systems	Response (%)
1 - Least advanced	0.5%
2	0.5%
3	5.9%
4	43.6%
5 - Most advanced	49.5%

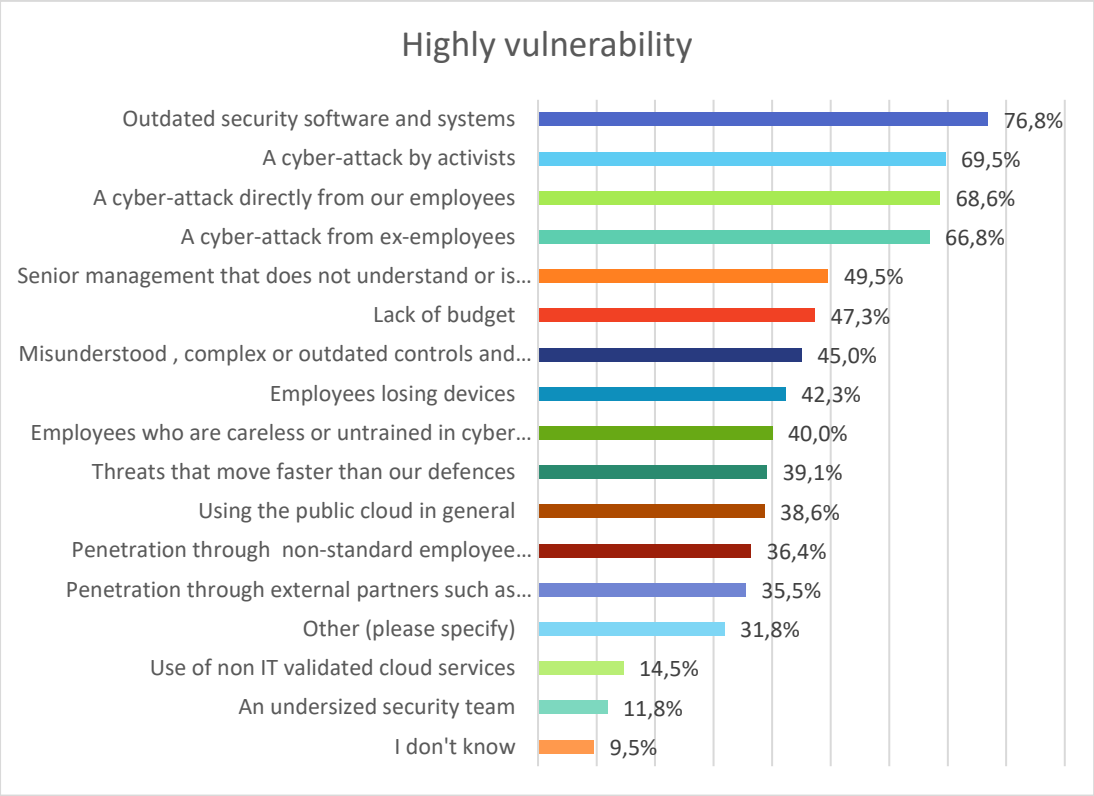
How complex is it securing multiple endpoints in your data centre?



How complex is it securing multiple endpoints in your data centre?	Response (%)
1 - Low complexity	2.7%
2	5.5%
3	24.1%
4	6.8%
5 - High complexity	57.3%

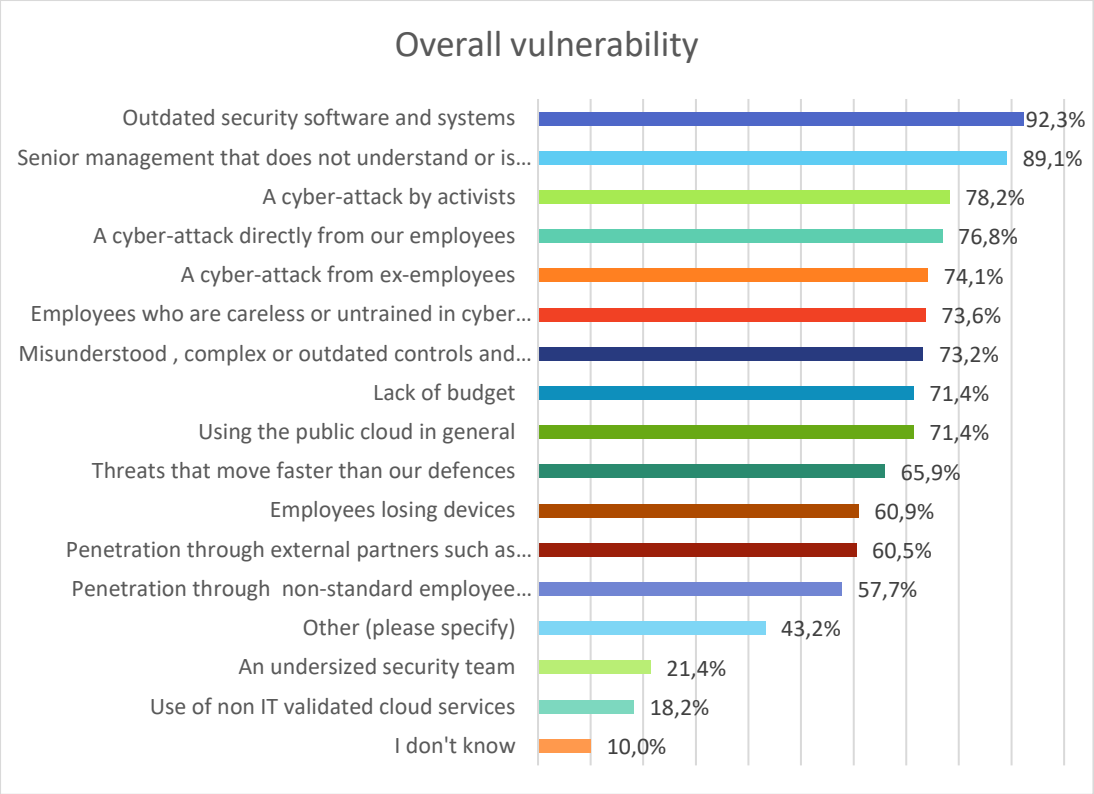
How vulnerable to cyberattack do the following make your organisation?

Most vulnerable (5 only)



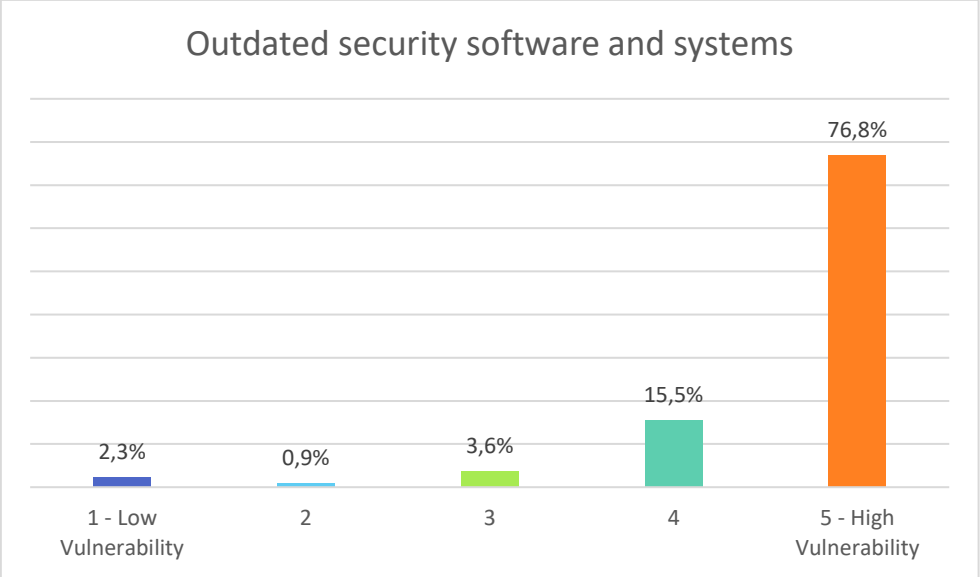
High vulnerability	Reponses (%)
Outdated security software and systems	76.8%
A cyber-attack by activists	69.5%
A cyber-attack directly from our employees	68.6%
A cyber-attack from ex-employees	66.8%
Senior management that does not understand or is uniformed about cyber risk or security	49.5%
Lack of budget	47.3%
Misunderstood, complex or outdated controls and processes	45.0%
Employees losing devices	42.3%
Employees who are careless or untrained in cyber security	40.0%
Threats that move faster than our defences	39.1%
Using the public cloud in general	38.6%
Penetration through non-standard employee devices (BYOD)	36.4%
Penetration through external partners such as suppliers or customers	35.5%
Other (please specify)	31.8%
Use of non-IT validated cloud services	14.5%
An undersized security team	11.8%
I don't know	9.5%

Overall vulnerability



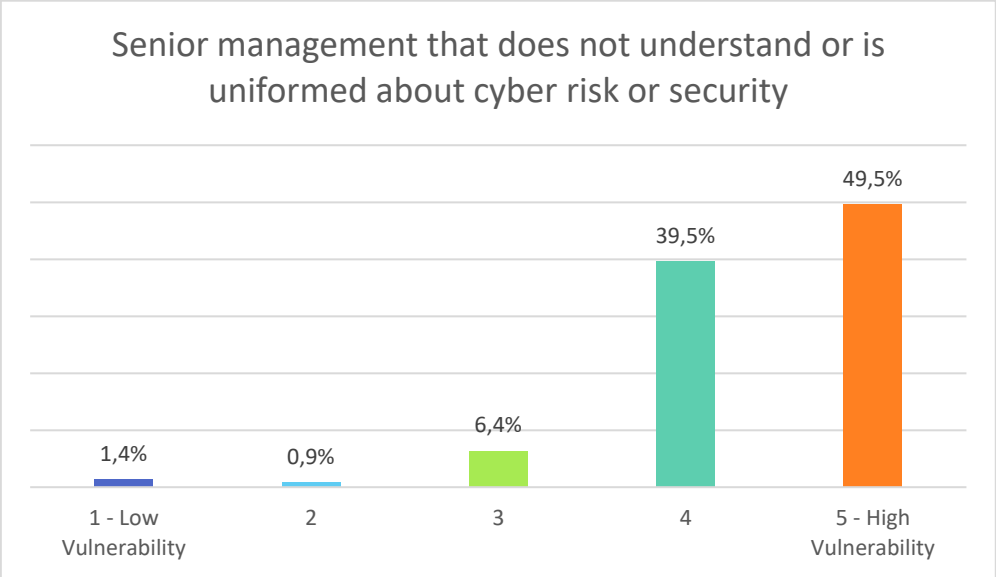
Overall vulnerability	**Responses (%)**
Outdated security software and systems	92.3%
Senior management that does not understand or is uniformed about cyber risk or security	89.1%
A cyber-attack by activists	78.2%
A cyber-attack directly from our employees	76.8%
A cyber-attack from ex-employees	74.1%
Employees who are careless or untrained in cyber security	73.6%
Misunderstood, complex or outdated controls and processes	73.2%
Lack of budget	71.4%
Using the public cloud in general	71.4%
Threats that move faster than our defences	65.9%
Employees losing devices	60.9%
Penetration through external partners such as suppliers or customers	60.5%
Penetration through non-standard employee devices (BYOD)	57.7%
Other (please specify)	43.2%
An undersized security team	21.4%
Use of non-IT validated cloud services	18.2%
I don't know	10.0%

Outdated security software and systems



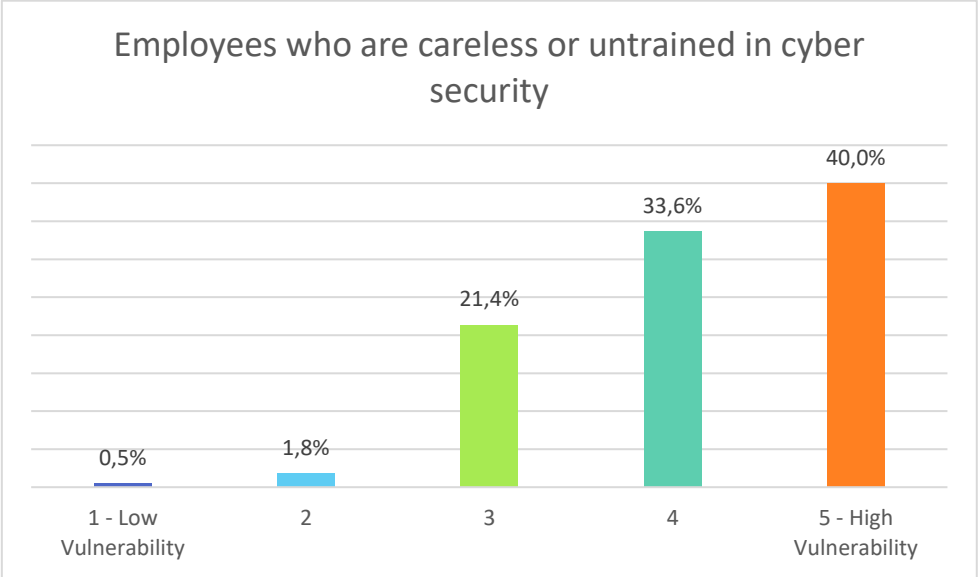
Outdated security software and systems	Responses (%)
1 - Low Vulnerability	2.3%
2	0.9%
3	3.6%
4	15.5%
5 - High Vulnerability	76.8%

Senior management that does not understand or is uniformed about cyber risk or security



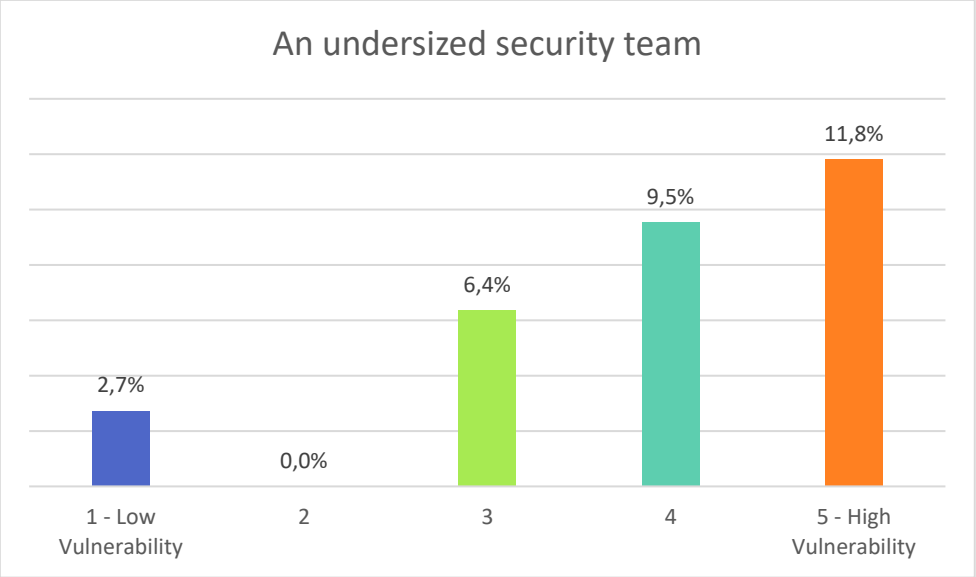
Senior management that does not understand or is uniformed about cyber risk or security	**Responses (%)**
1 - Low Vulnerability	1.4%
2	0.9%
3	6.4%
4	39.5%
5 - High Vulnerability	49.5%

Employees who are careless or untrained in cyber security



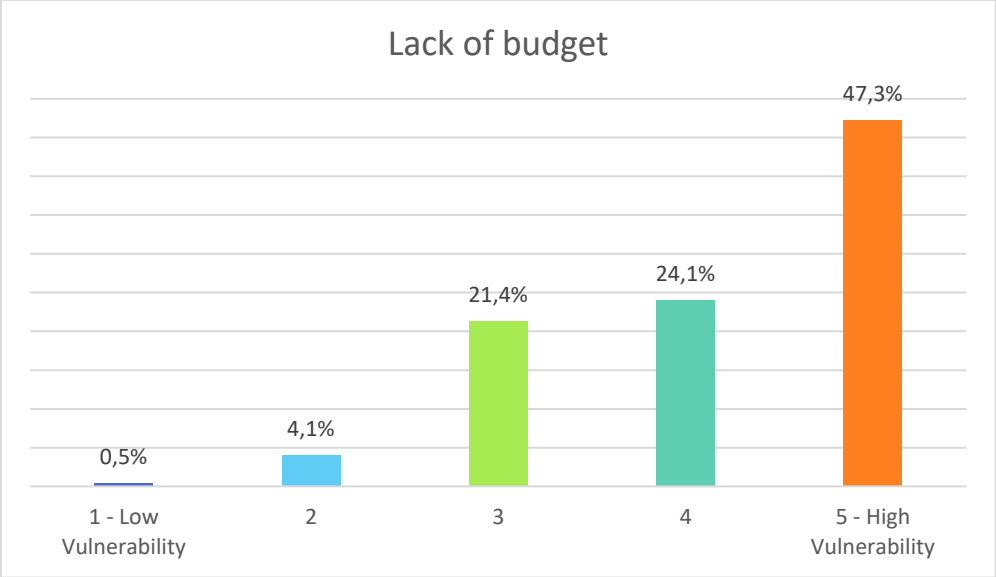
Employees who are careless or untrained in cyber security	**Responses (%)**
1 - Low Vulnerability	0.5%
2	1.8%
3	21.4%
4	33.6%
5 - High Vulnerability	40.0%

An undersized security team



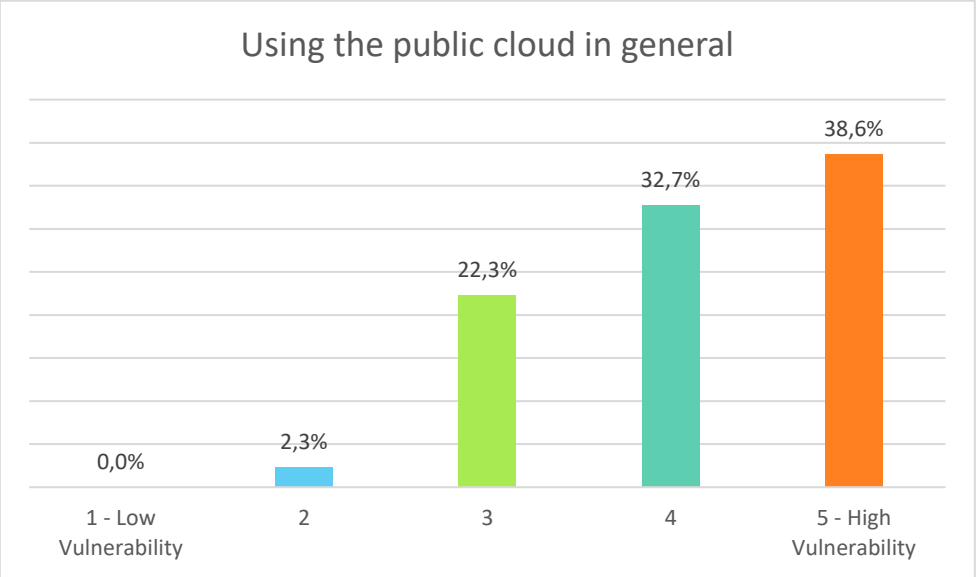
An undersized security team	Responses (%)
1 - Low Vulnerability	2.7%
2	0.0%
3	6.4%
4	9.5%
5 - High Vulnerability	11.8%

Lack of budget



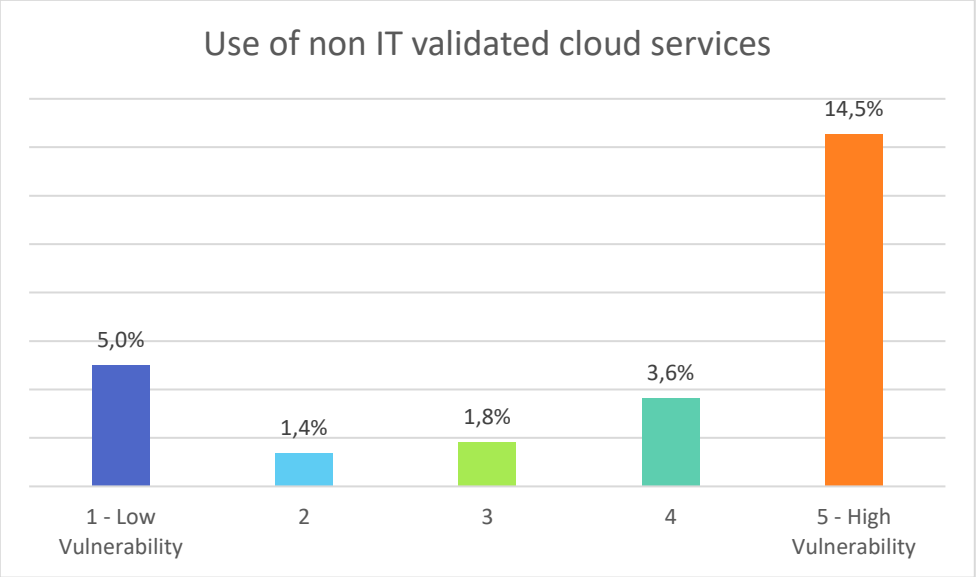
Lack of budget	**Responses (%)**
1 - Low Vulnerability	0.5%
2	4.1%
3	21.4%
4	24.1%
5 - High Vulnerability	47.3%

Using the public cloud in general



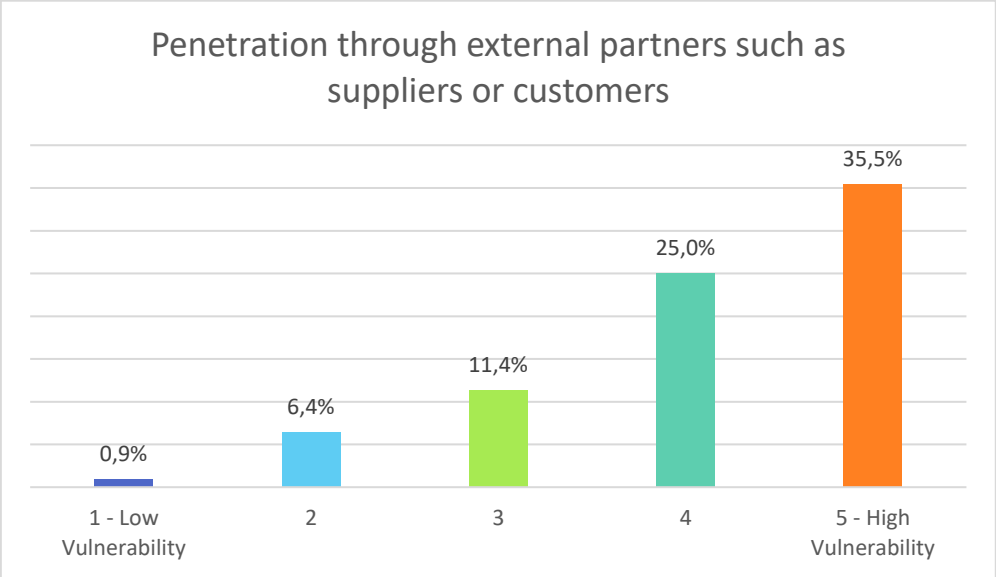
Using the public cloud in general	Responses (%)
1 - Low Vulnerability	0.0%
2	2.3%
3	22.3%
4	32.7%
5 - High Vulnerability	38.6%

Use of non-IT validated cloud services



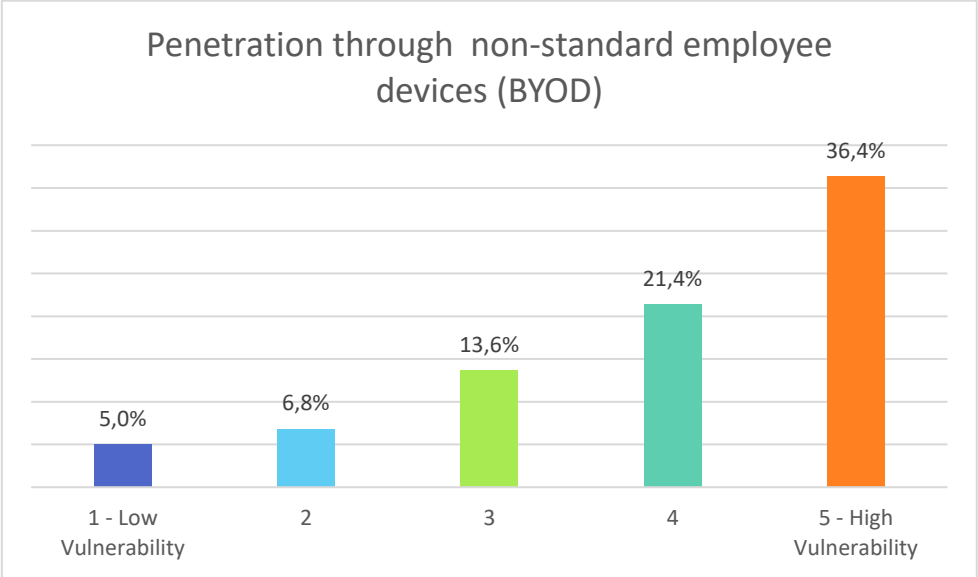
Use of non-IT validated cloud services	Responses (%)
1 - Low Vulnerability	5.0%
2	1.4%
3	1.8%
4	3.6%
5 - High Vulnerability	14.5%

Penetration through external partners such as suppliers or customers



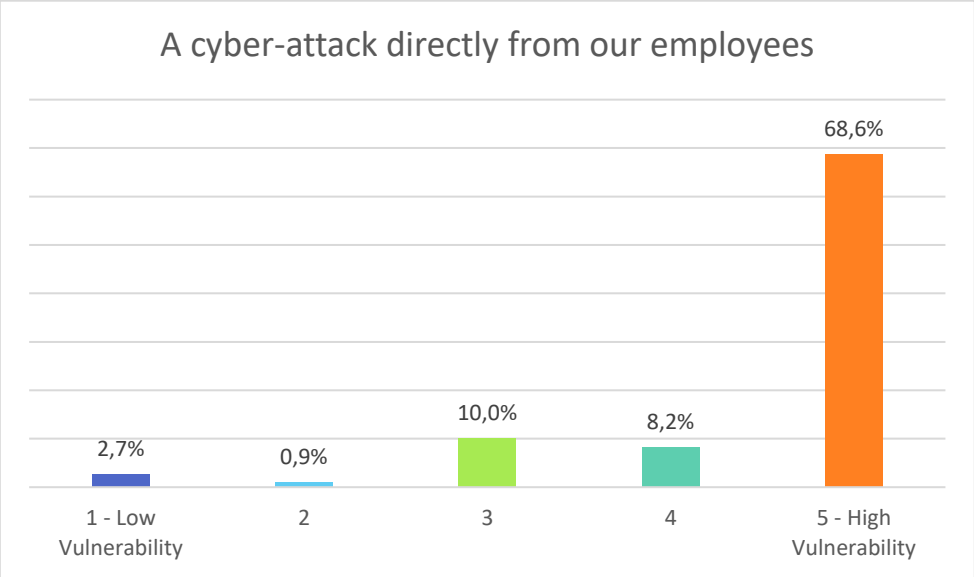
Penetration through external partners such as suppliers or customers	**Responses (%)**
1 - Low Vulnerability	0.9%
2	6.4%
3	11.4%
4	25.0%
5 - High Vulnerability	35.5%

Penetration through non-standard employee devices (BYOD)



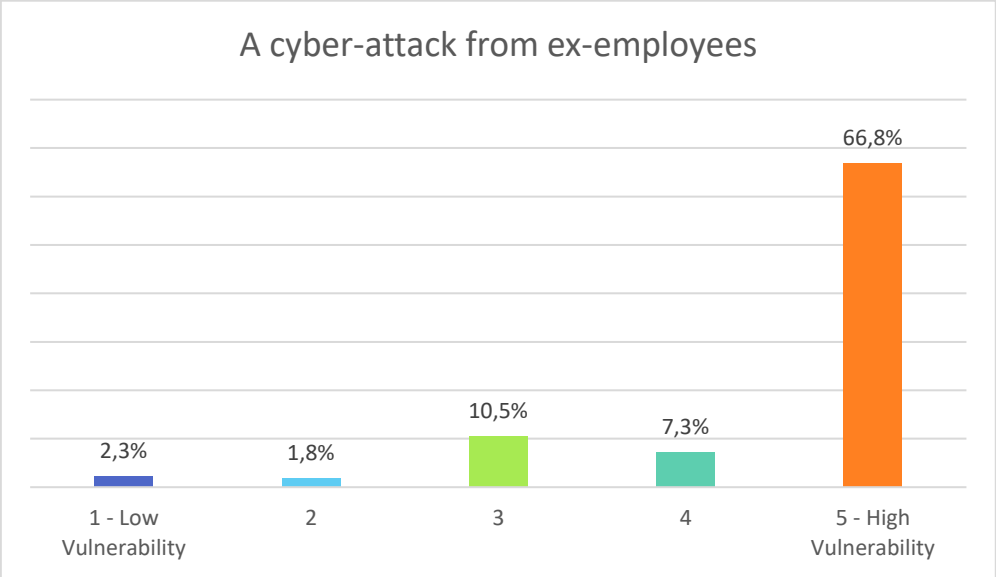
Penetration through non-standard employee devices (BYOD)	**Responses (%)**
1 - Low Vulnerability	5.0%
2	6.8%
3	13.6%
4	21.4%
5 - High Vulnerability	36.4%

A cyber-attack directly from our employees



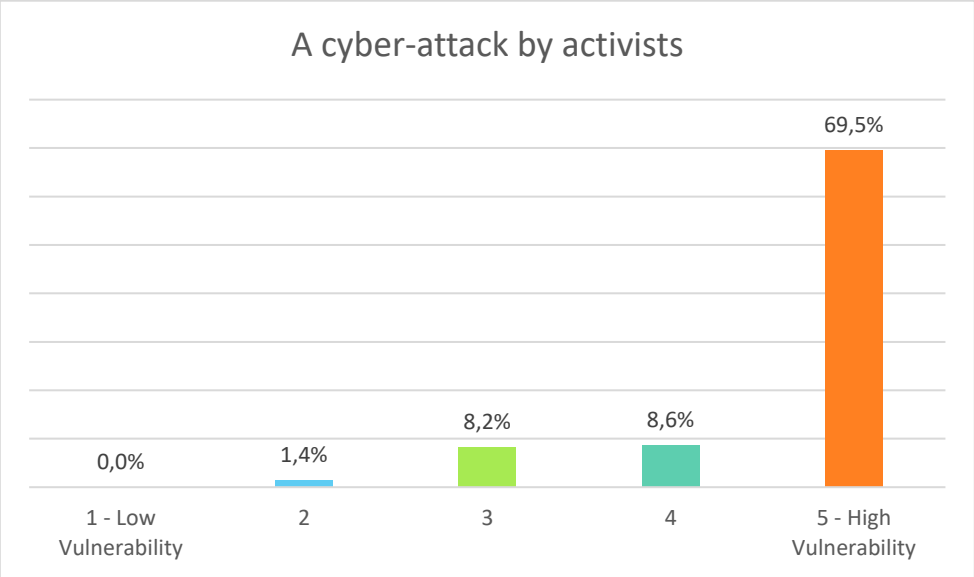
A cyber-attack directly from our employees	**Responses (%)**
1 - Low Vulnerability	2.7%
2	0.9%
3	10.0%
4	8.2%
5 - High Vulnerability	68.6%

A cyber-attack from ex-employees



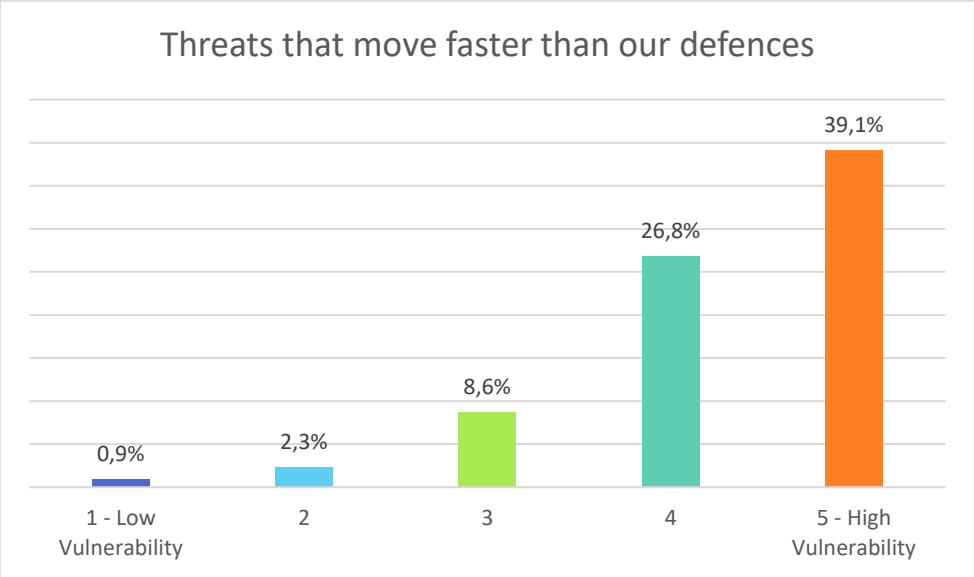
A cyber-attack from ex-employees	Responses (%)
1 - Low Vulnerability	2.3%
2	1.8%
3	10.5%
4	7.3%
5 - High Vulnerability	66.8%

A cyber-attack by activists



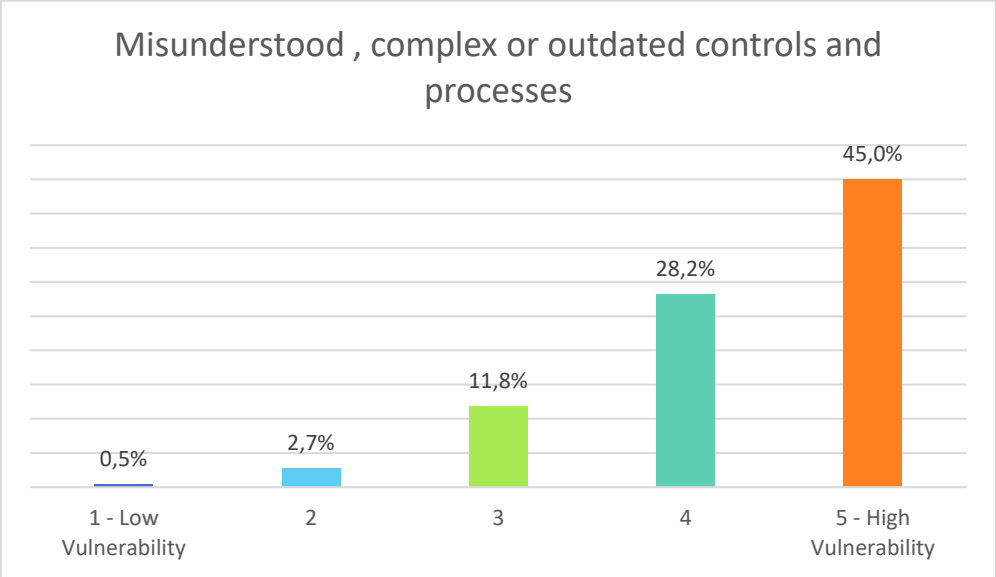
A cyber-attack by activists	Responses (%)
1 - Low Vulnerability	0.0%
2	1.4%
3	8.2%
4	8.6%
5 - High Vulnerability	69.5%

Threats that move faster than our defences



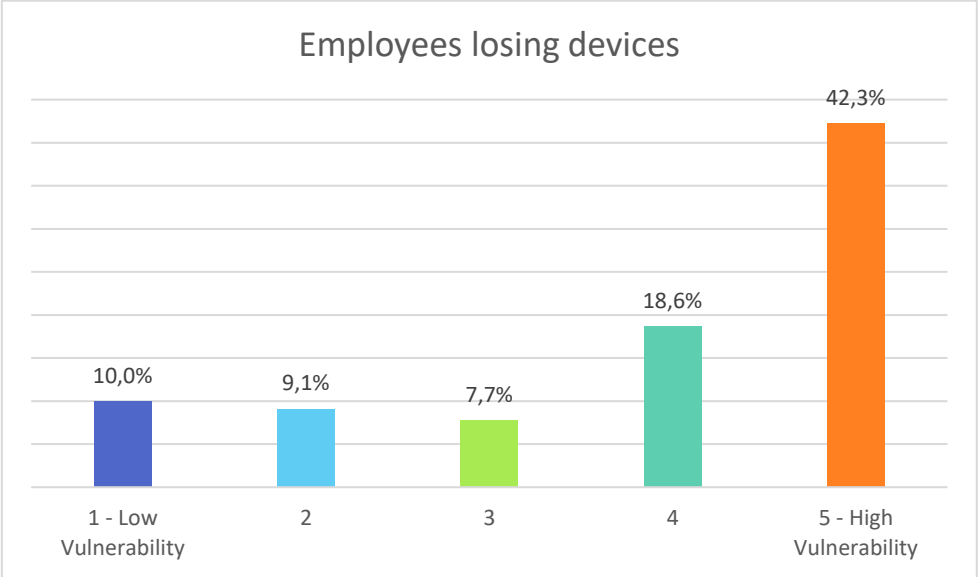
Threats that move faster than our defences	**Responses (%)**
1 - Low Vulnerability	0.9%
2	2.3%
3	8.6%
4	26.8%
5 - High Vulnerability	39.1%

Misunderstood, complex or outdated controls and processes



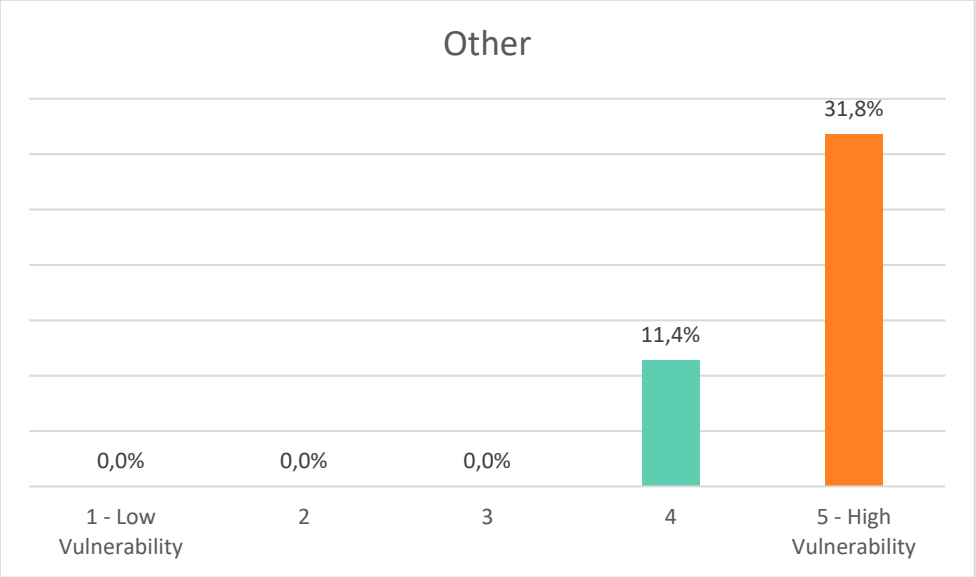
Misunderstood, complex or outdated controls and processes	**Responses (%)**
1 - Low Vulnerability	0.5%
2	2.7%
3	11.8%
4	28.2%
5 - High Vulnerability	45.0%

Employees losing devices



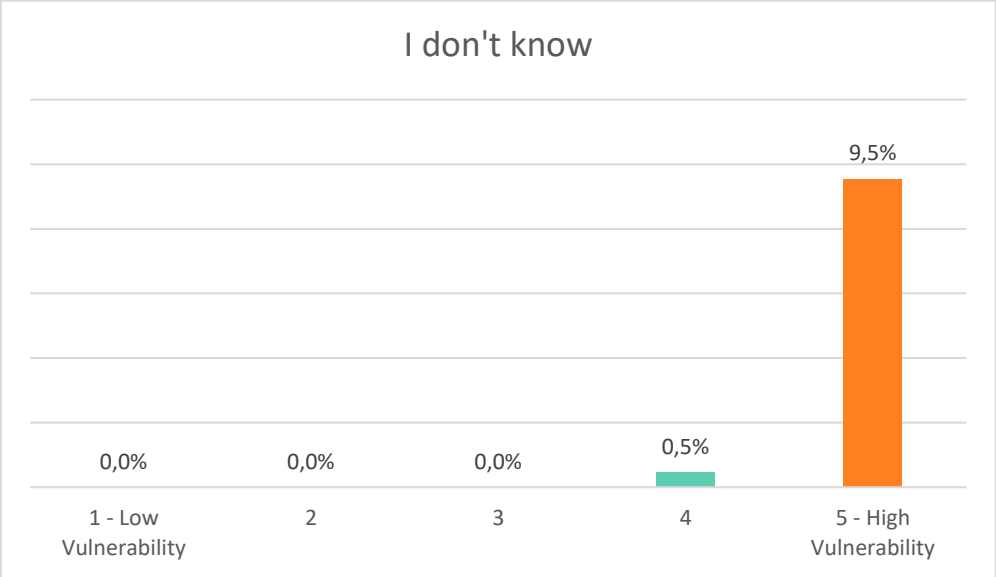
Employees losing devices	Responses (%)
1 - Low Vulnerability	10.0%
2	9.1%
3	7.7%
4	18.6%
5 - High Vulnerability	42.3%

Other



Other	Responses (%)
1 - Low Vulnerability	0.0%
2	0.0%
3	0.0%
4	11.4%
5 - High Vulnerability	31.8%

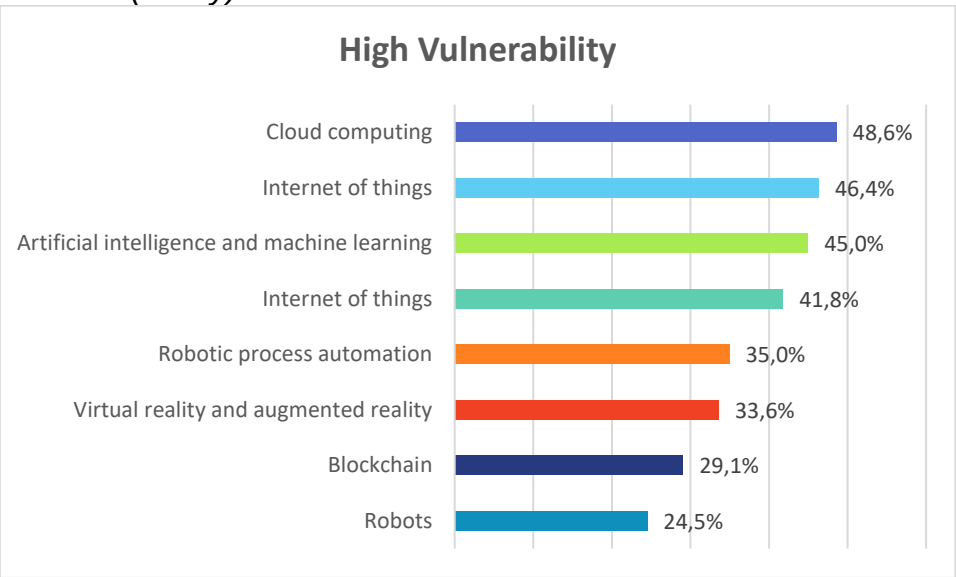
I don't know



I don’t know	Responses (%)
1 - Low Vulnerability	0.0%
2	0.0%
3	0.0%
4	0.5%
5 - High Vulnerability	9.5%

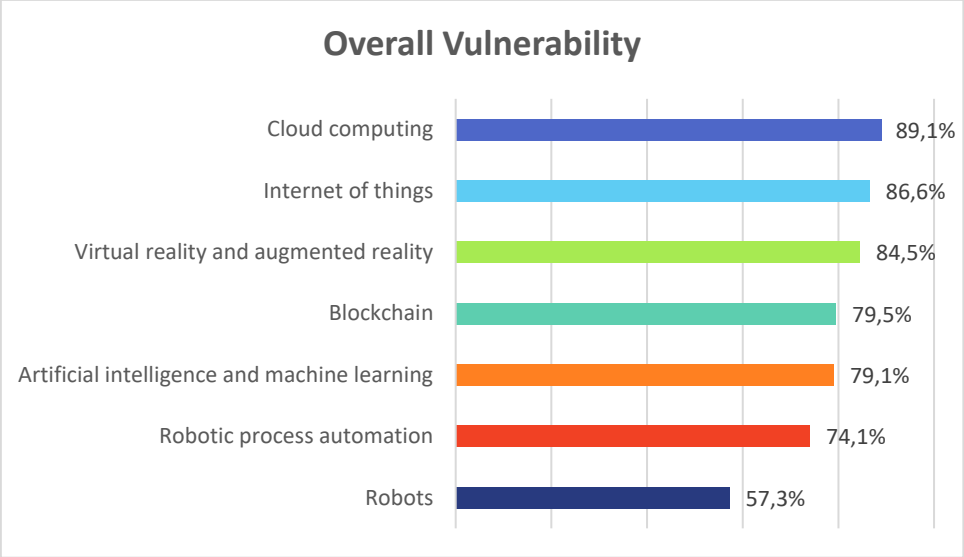
How much of a threat do you believe these emerging technologies pose to your organisation in terms of vulnerability to cyber-attacks?

Highly vulnerable (5 only)



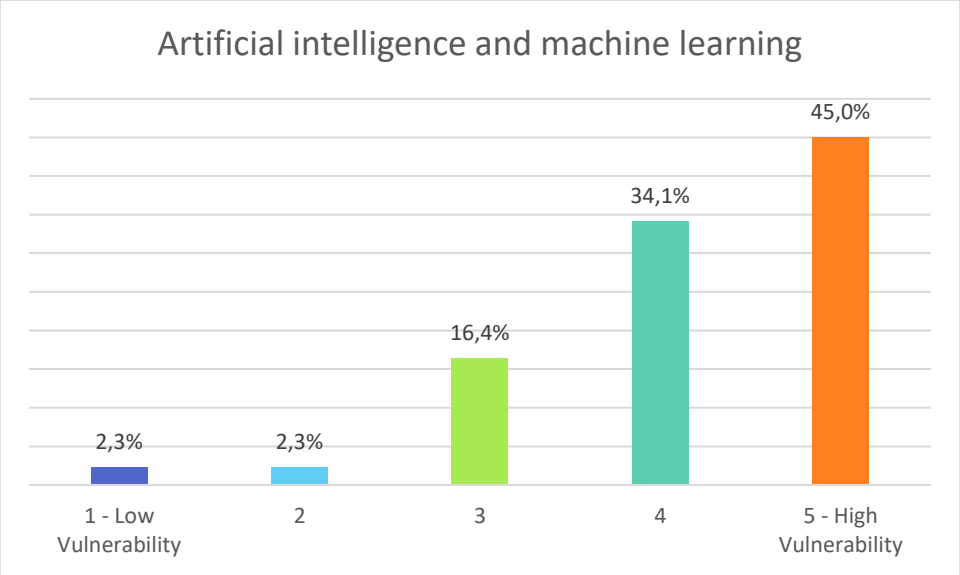
High vulnerability	Responses (%)
Cloud computing	48.6%
Artificial intelligence and machine learning	45.0%
Internet of things	44.1%
Robotic process automation	35.0%
Virtual reality and augmented reality	33.6%
Blockchain	29.1%
Robots	24.5%

Overall vulnerable (4/5 combined)



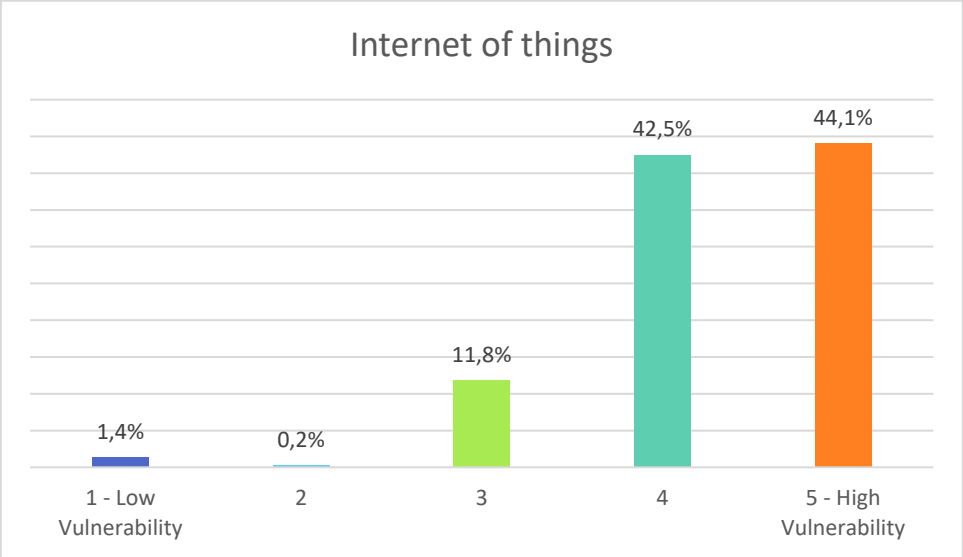
Overall vulnerability	**Response (%)**
Cloud computing	89.1%
Internet of things	86.6%
Virtual reality and augmented reality	84.5%
Blockchain	79.5%
Artificial intelligence and machine learning	79.1%
Robotic process automation	74.1%
Robots	57.3%

Artificial intelligence and machine learning



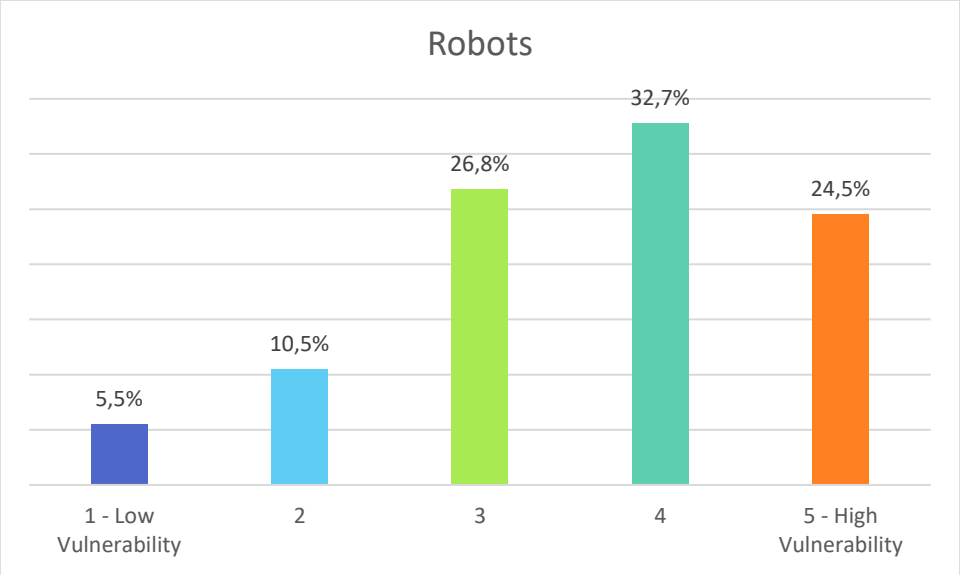
Artificial intelligence and machine learning	Responses (%)
1 - Low Vulnerability	2.3%
2	2.3%
3	16.4%
4	34.1%
5 - High Vulnerability	45.0%

Internet of things



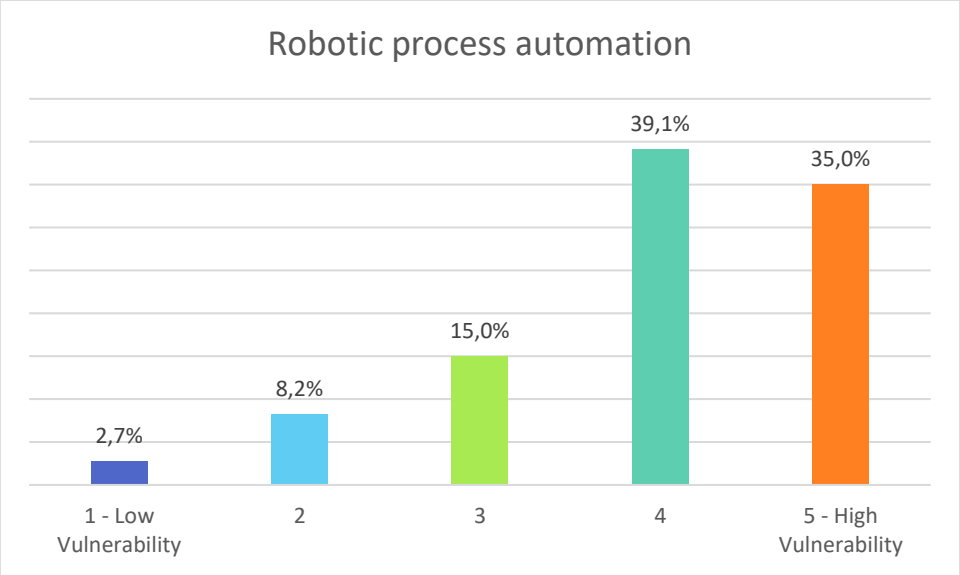
Internet of Things	Responses (%)
1 - Low Vulnerability	1.4%
2	0.2%
3	11.8%
4	42.5%
5 - High Vulnerability	44.1%

Robots



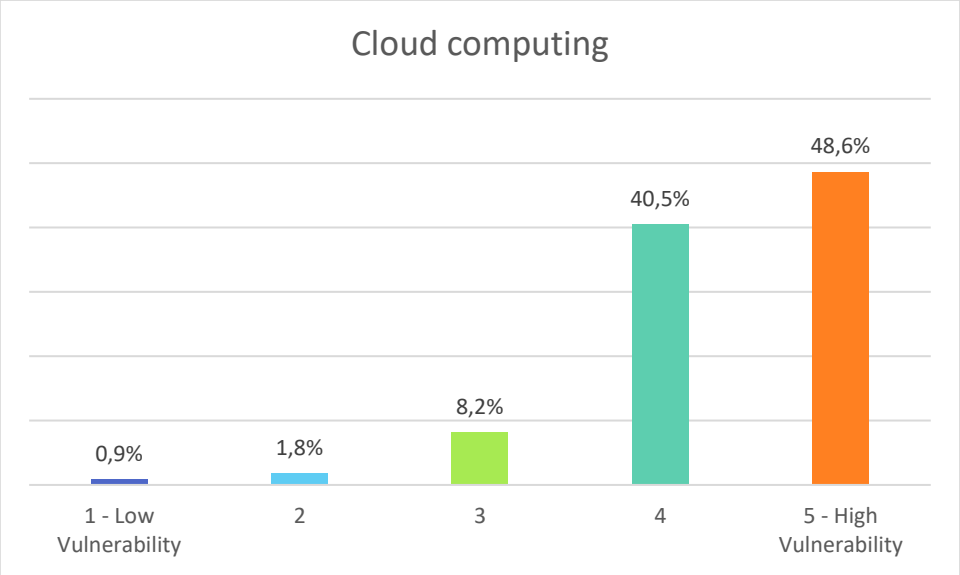
Robots	Responses (%)
1 - Low Vulnerability	5.5%
2	10.5%
3	26.8%
4	32.7%
5 - High Vulnerability	24.5%

Robotic process automation



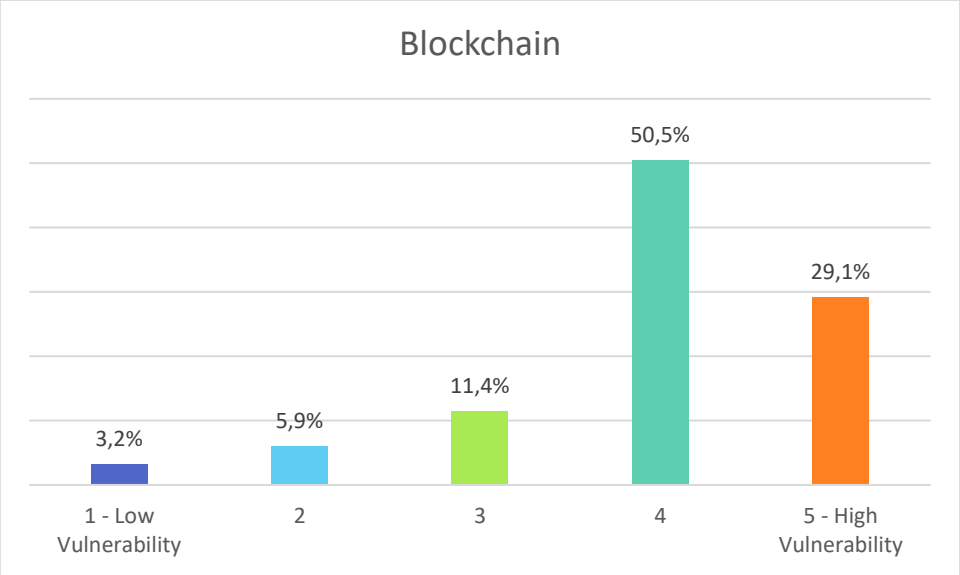
Robotic process automation	Responses (%)
1 - Low Vulnerability	2.7%
2	8.2%
3	15.0%
4	39.1%
5 - High Vulnerability	35.0%

Cloud computing



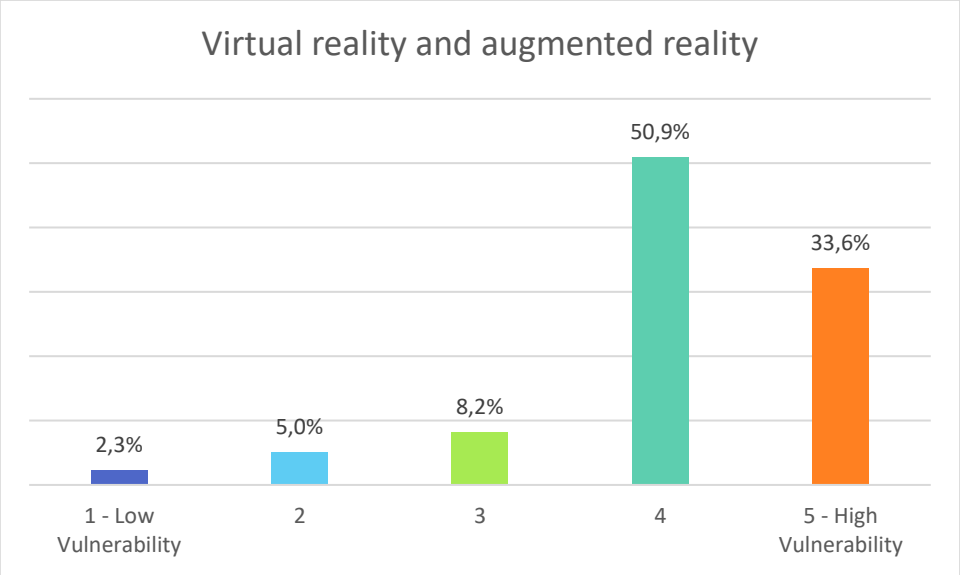
Cloud computing	Responses (%)
1 - Low Vulnerability	0.9%
2	1.8%
3	8.2%
4	40.5%
5 - High Vulnerability	48.6%

Blockchain



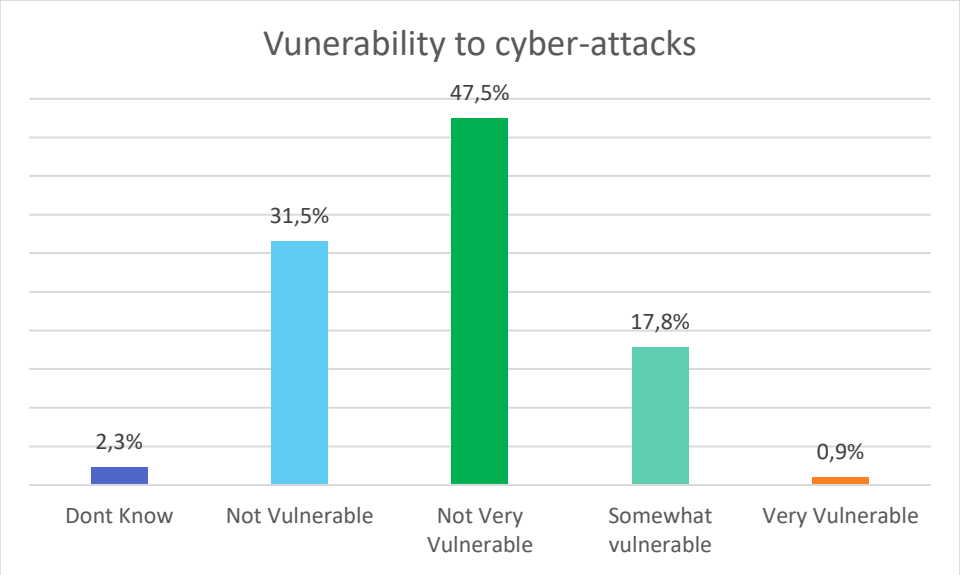
Blockchain	Responses (%)
1 - Low Vulnerability	3.2%
2	5.9%
3	11.4%
4	50.5%
5 - High Vulnerability	29.1%

Virtual reality and augmented reality



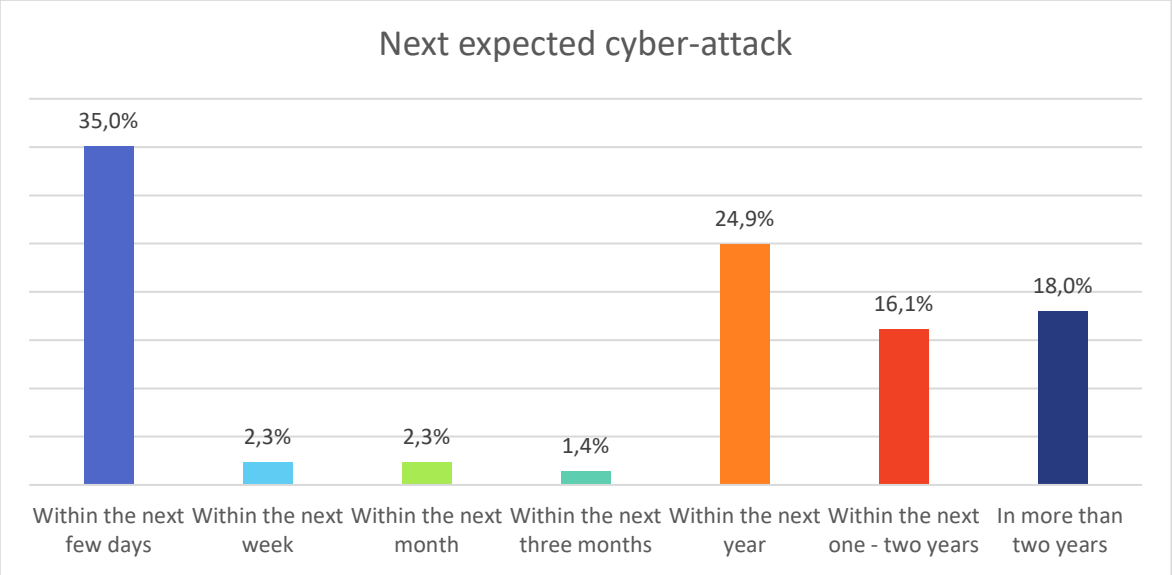
VR/AR	Responses (%)
1 - Low Vulnerability	2.3%
2	5.0%
3	8.2%
4	50.9%
5 - High Vulnerability	33.6%

How vulnerable is your organisation to cyber-attacks?



How vulnerable do you believe your organization is to cyber-attacks?	Responses (%)
Don't Know	2.3%
Not Vulnerable	31.5%
Not Very Vulnerable	47.5%
Somewhat vulnerable	17.8%
Very Vulnerable	0.9%

When do you expect to have a cyber-attack on your organisation?

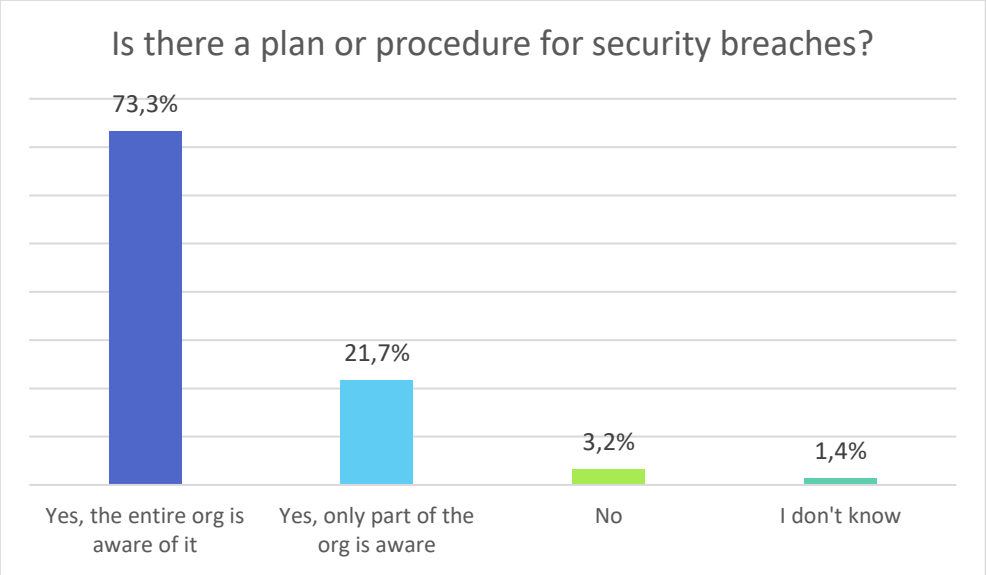


What time frame is the most likely for your organisation to experience a serious cyber-attack?	Responses (%)
Within the next few days	35.0%
Within the next week	2.3%
Within the next month	2.3%
Within the next three months	1.4%
Within the next year	24.9%
Within the next one - two years	16.1%
In more than two years	18.0%

How quickly will your organisation know that a cyber-attack has taken place?

How quickly will your organisation know that a cyber-attack has taken place?	Responses (%)
Within minutes	56.7%
Within hours	33.6%
Within half a day	1.8%
Within 24 hours	1.4%
Within the next few days	1.8%
Within the week	0.5%
Within three months	0.9%
Within a year	2.3%
It will never realise	0.9%

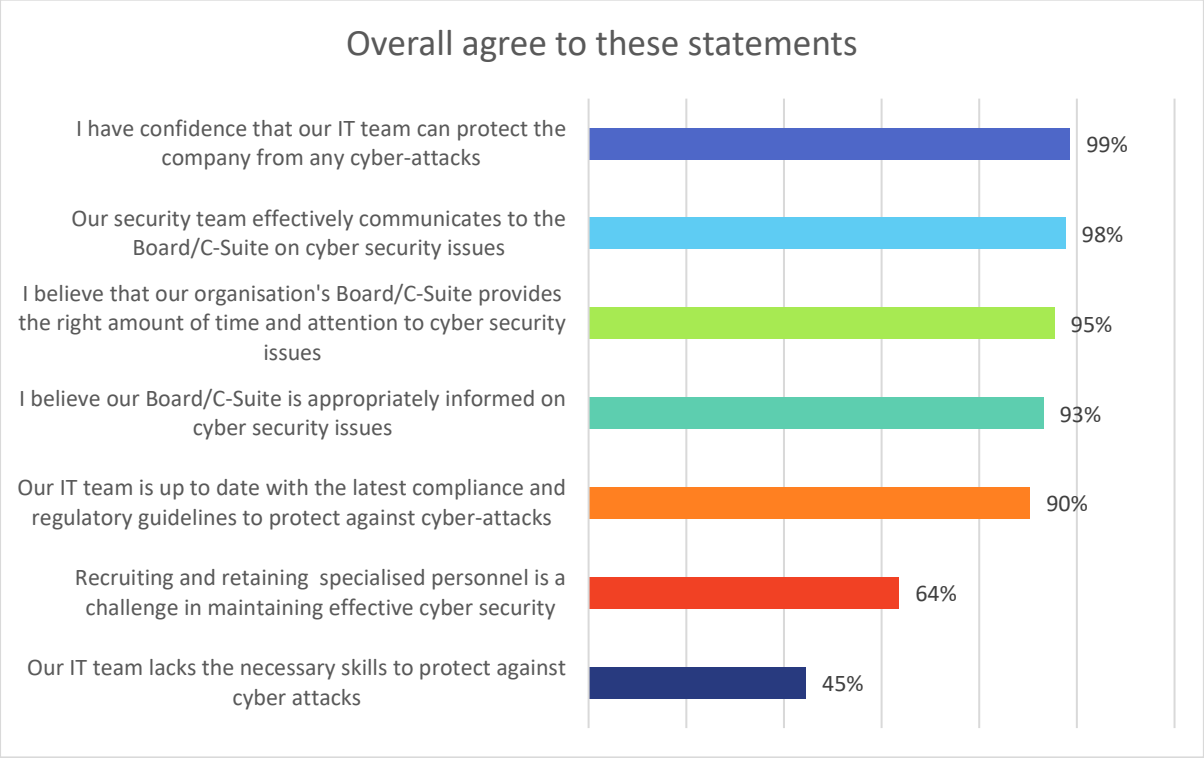
Is there a plan or procedure in place to deal with security breaches?



Is there a plan or procedure in place to deal with security breaches?	Respondents (%)
Yes, the entire org is aware of it	73.3%
Yes, only part of the org is aware	21.7%
No	3.2%
I don't know	1.4%

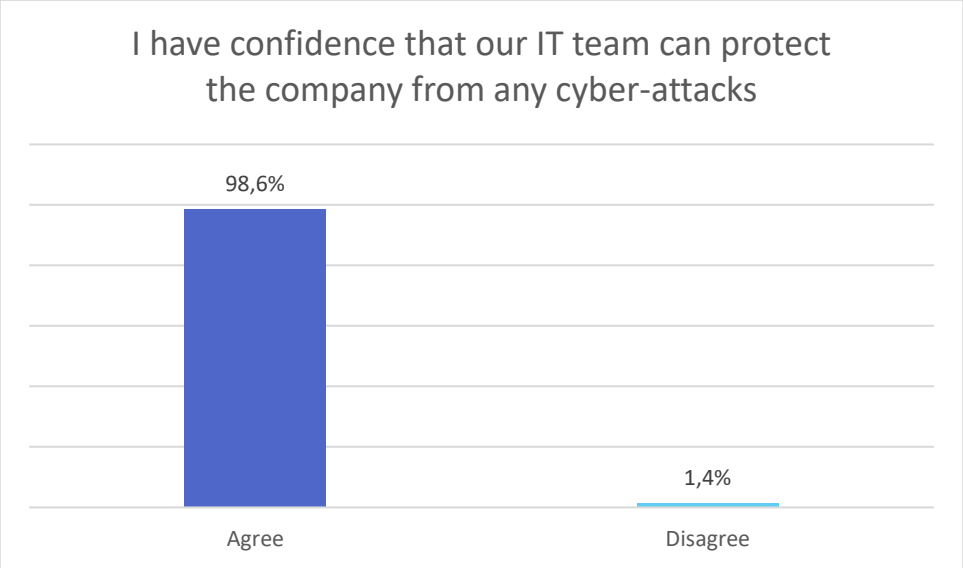
Do you agree with the following statements, assessing your organisations, current cyber security needs?

Overall agree to these statements



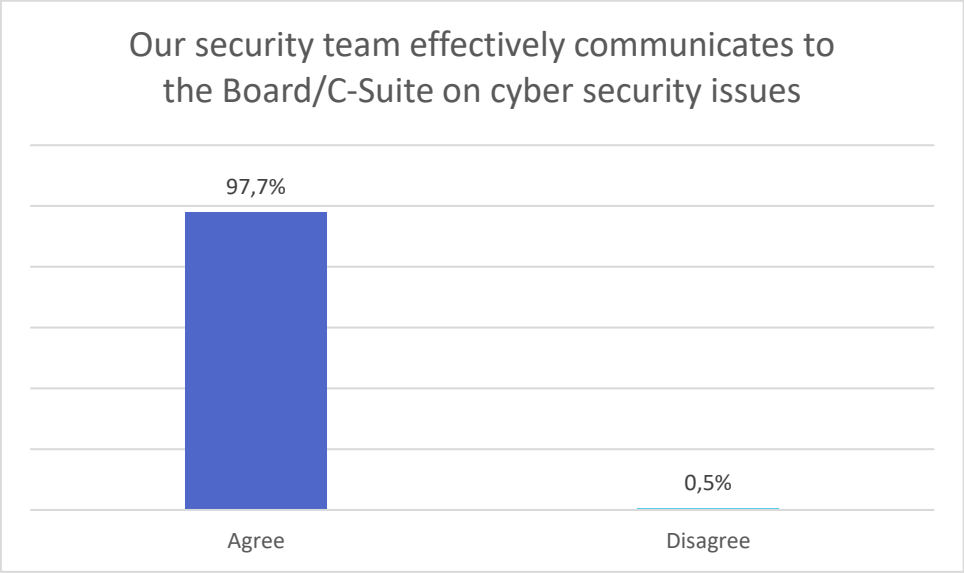
Overall Agree	Responses (%)
I have confidence that our IT team can protect the company from any cyber-attacks	99%
Our security team effectively communicates to the Board/C-Suite on cyber security issues	98%
I believe that our organisation's Board/C-Suite provides the right amount of time and attention to cyber security issues	95%
I believe our Board/C-Suite is appropriately informed on cyber security issues	93%
Our IT team is up to date with the latest compliance and regulatory guidelines to protect against cyber-attacks	90%
Recruiting and retaining specialised personnel is a challenge in maintaining effective cyber security	64%
Our IT team lacks the necessary skills to protect against cyber attacks	45%

I have confidence that our IT team can protect the company from any cyber-attacks



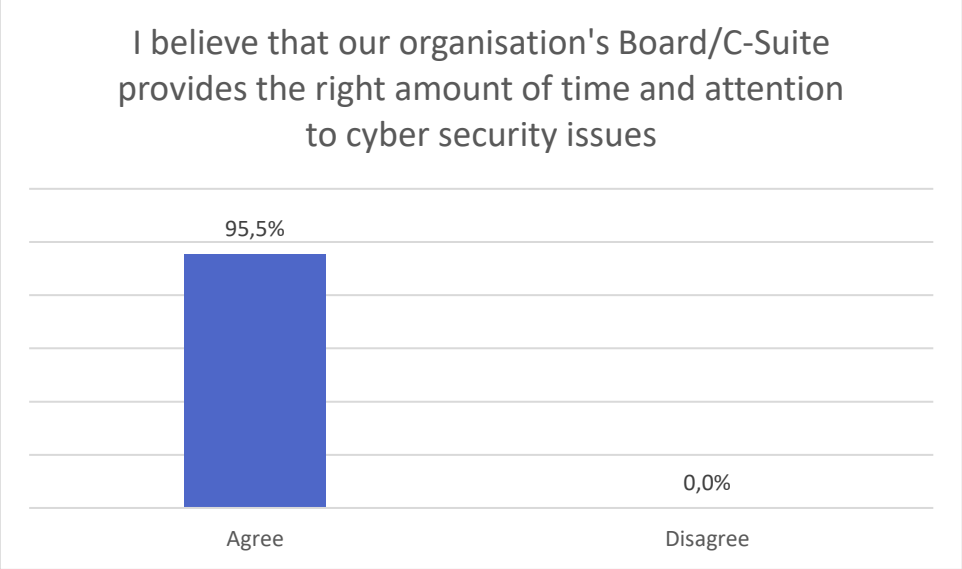
I have confidence that our IT team can protect the company from any cyber-attacks	**Respondents (%)**
Agree	98.6%
Disagree	1.4%

Our security team effectively communicates to the Board/C-Suite on cyber security issues



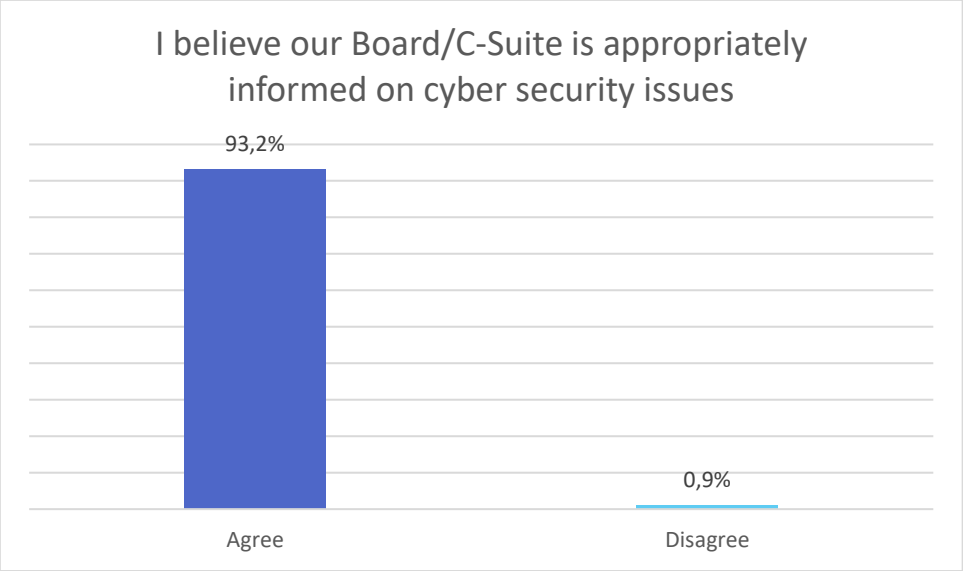
Our security team effectively communicates to the Board/C-Suite on cyber security issues	**Respondents (%)**
Agree	97.7%
Disagree	0.5%

I believe that our organisation's Board/C-Suite provides the right amount of time and attention to cyber security issues



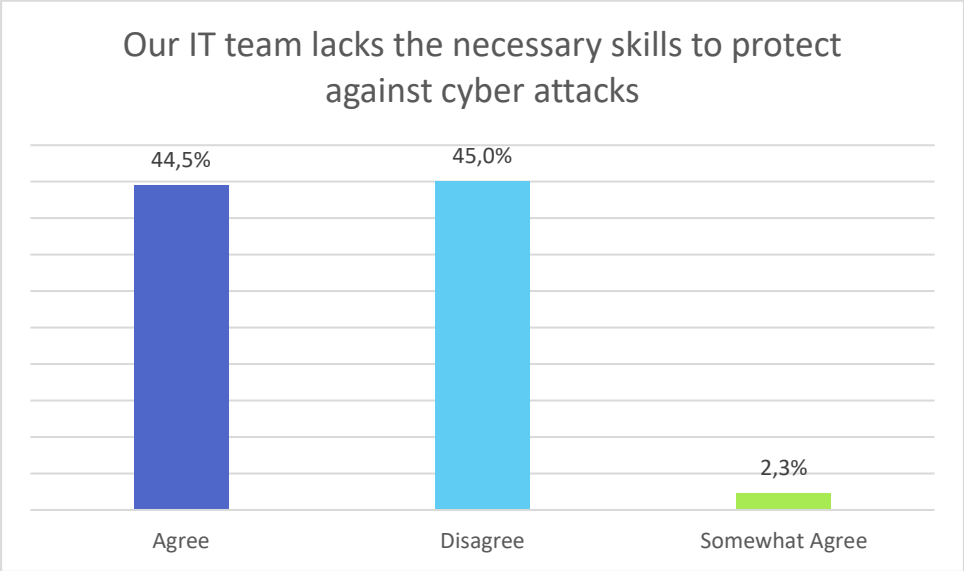
I believe that our organisation's Board/C-Suite provides the right amount of time and attention to cyber security issues	**Respondents (%)**
Agree	95.5%
Disagree	0.0%

I believe our Board/C-Suite is appropriately informed on cyber security issues



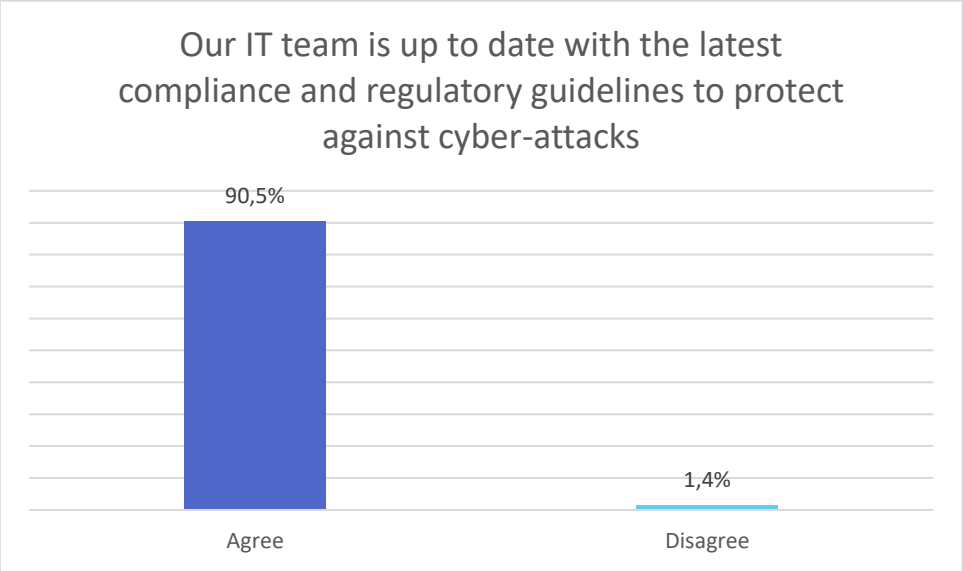
I believe our Board/C-Suite is appropriately informed on cyber security issues	**Respondents (%)**
Agree	93.2%
Disagree	0.9%

Our IT team lacks the necessary skills to protect against cyber attacks



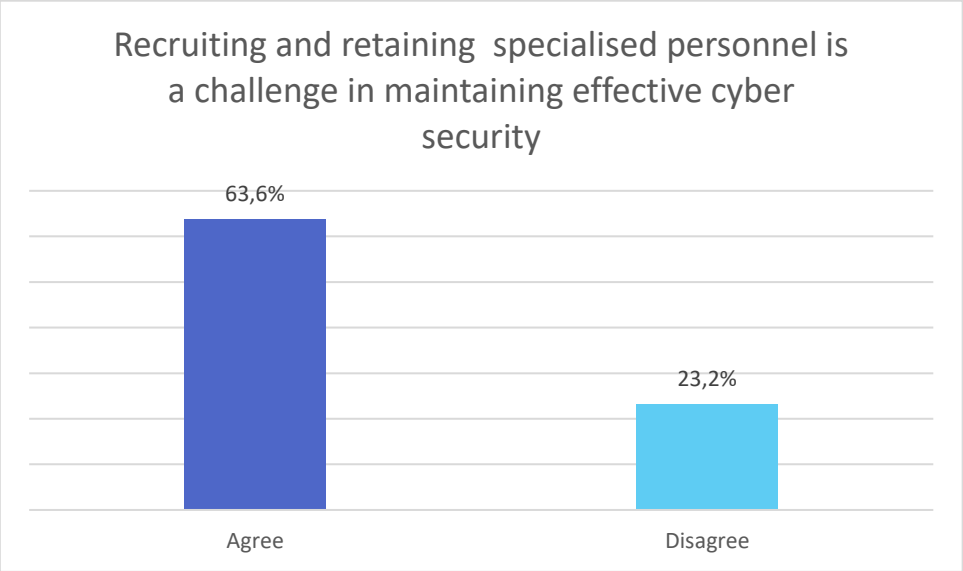
Our IT team lacks the necessary skills to protect against cyber attacks	**Respondents (%)**
Agree	44.5%
Disagree	45.0%
Somewhat Agree	2.3%

Our IT team is up to date with the latest compliance and regulatory guidelines to protect against cyber-attacks



Our IT team is up to date with the latest compliance and regulatory guidelines to protect against cyber-attacks	**Respondents (%)**
Agree	90.5%
Disagree	1.4%

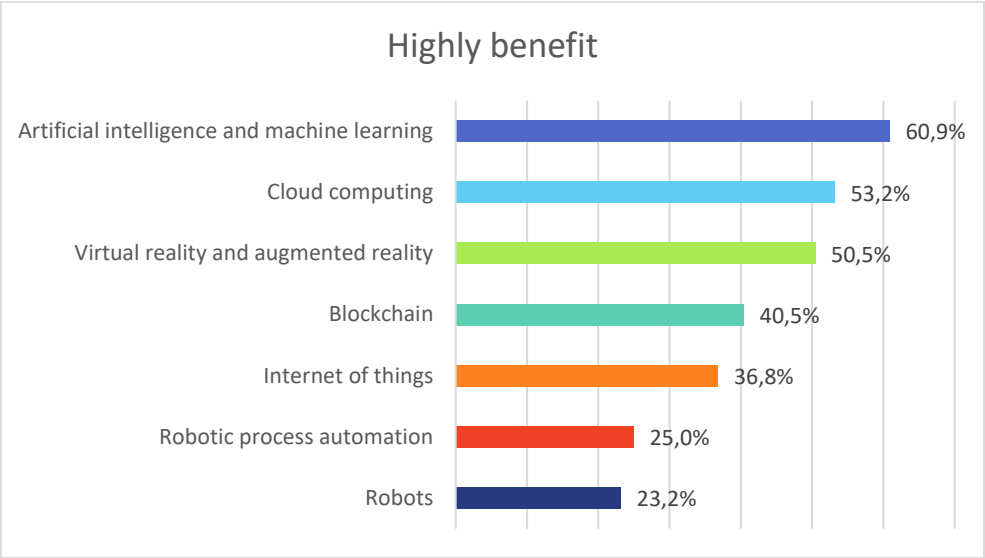
Recruiting and retaining specialised personnel is a challenge in maintaining effective cyber security



Recruiting and retaining specialised personnel is a challenge in maintaining effective cyber security	**Respondents (%)**
Agree	63.6%
Disagree	23.2%

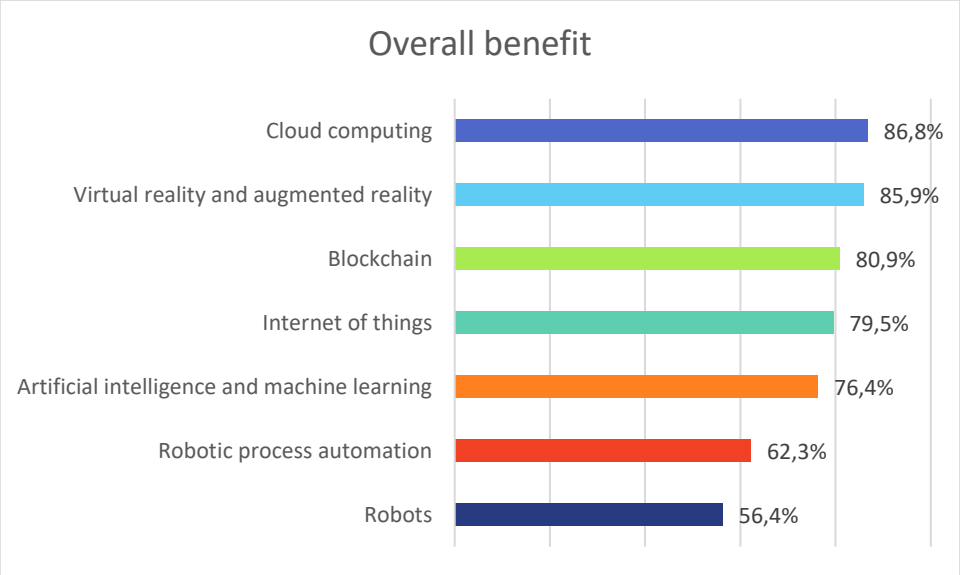
How strongly do you believe these emerging technologies will benefit your organisation in protecting against cyber-attacks?

Highly benefit



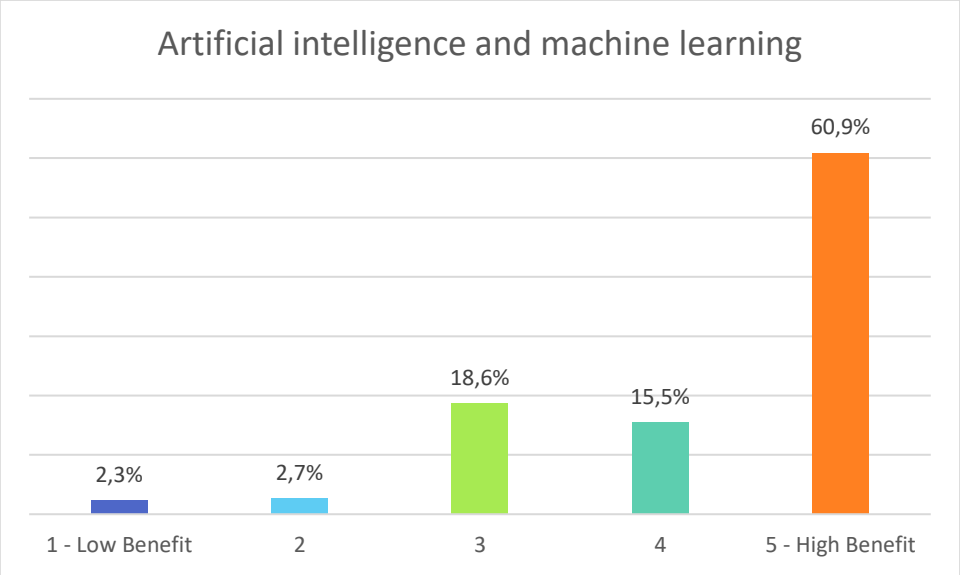
Highly benefit	Responses (%)
Artificial intelligence and machine learning	60.9%
Cloud computing	53.2%
Virtual reality and augmented reality	50.5%
Blockchain	40.5%
Internet of things	36.8%
Robotic process automation	25.0%
Robots	23.2%

Overall benefit



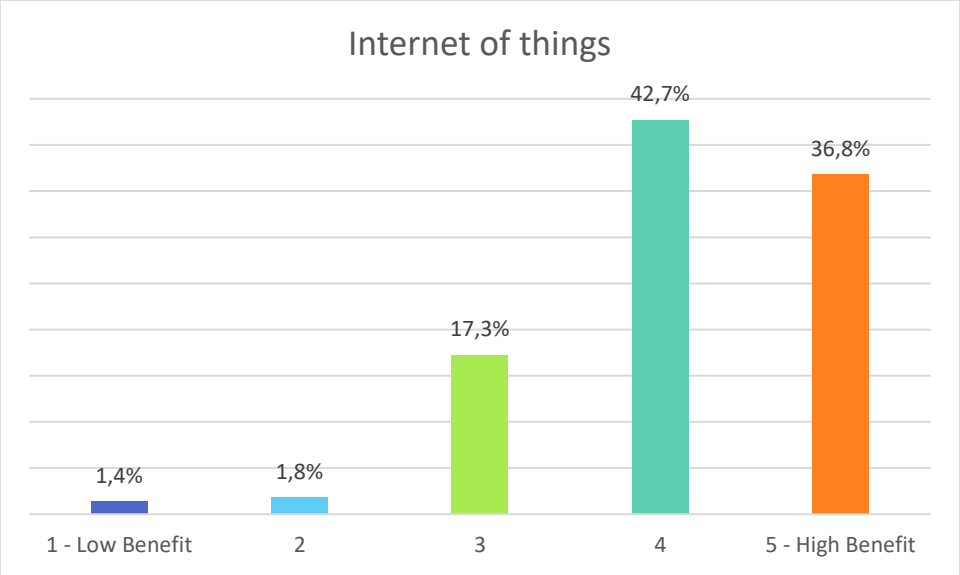
Overall benefit	**Responses (%)**
Cloud computing	86.8%
Virtual reality and augmented reality	85.9%
Blockchain	80.9%
Internet of things	79.5%
Artificial intelligence and machine learning	76.4%
Robotic process automation	62.3%
Robots	56.4%

Artificial intelligence and machine learning



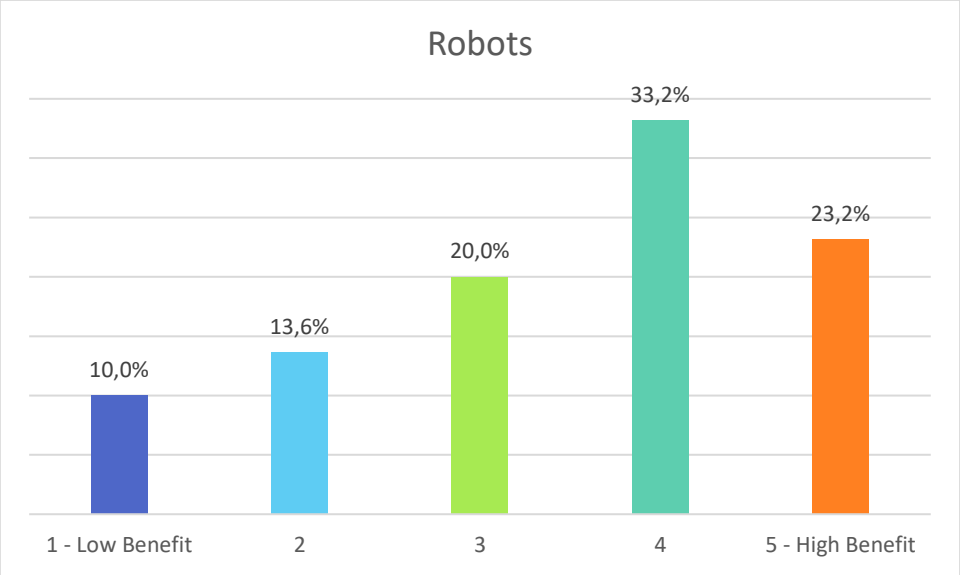
Artificial intelligence and machine learning	Responses (%)
1 - Low Benefit	2.3%
2	2.7%
3	18.6%
4	15.5%
5 - High Benefit	60.9%

Internet of things



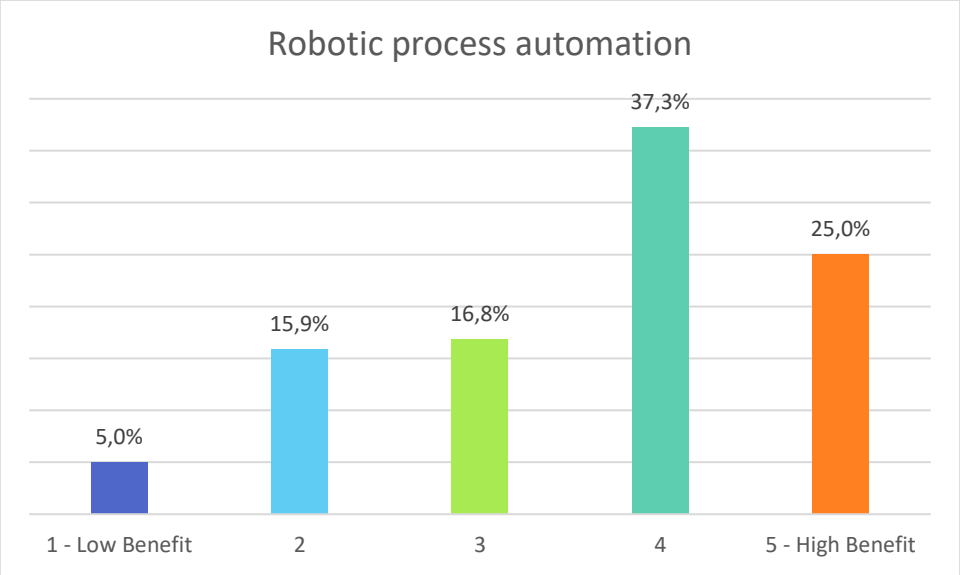
Internet of Things	Responses (%)
1 - Low Benefit	1.4%
2	1.8%
3	17.3%
4	42.7%
5 - High Benefit	36.8%

Robots



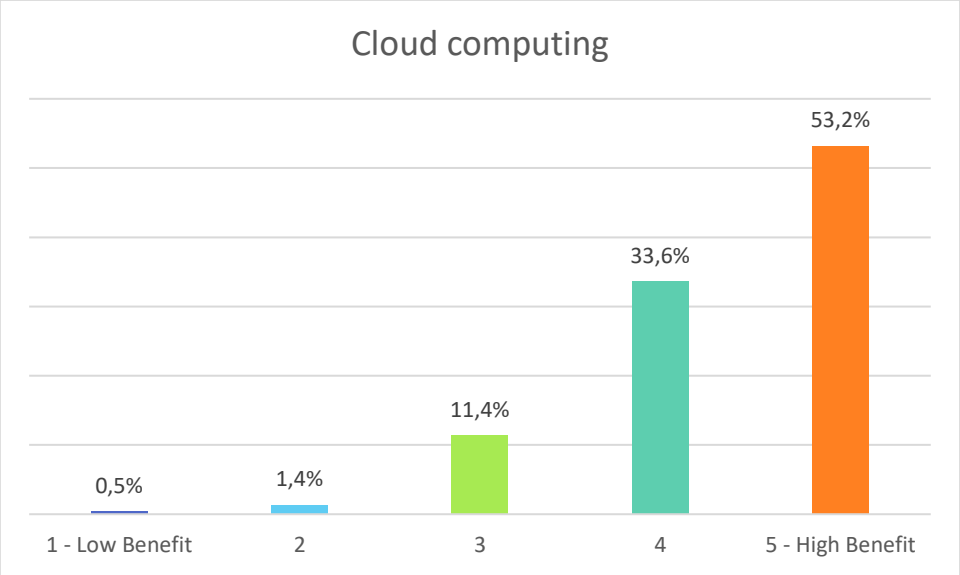
Robots	Responses (%)
1 - Low Benefit	10.0%
2	13.6%
3	20.0%
4	33.2%
5 - High Benefit	23.2%

Robotic process automation



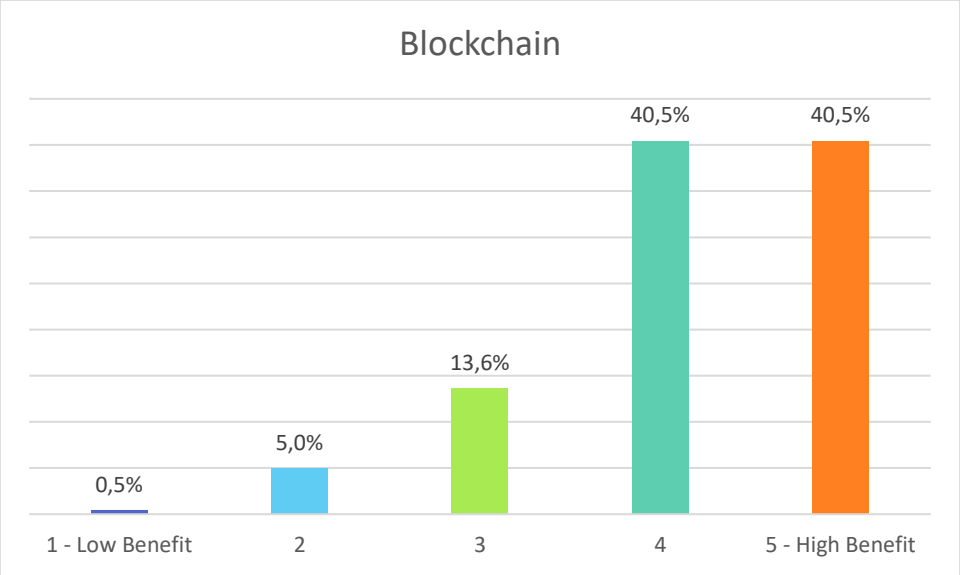
Robotic process automation	Responses (%)
1 - Low Benefit	5.0%
2	15.9%
3	16.8%
4	37.3%
5 - High Benefit	25.0%

Cloud computing



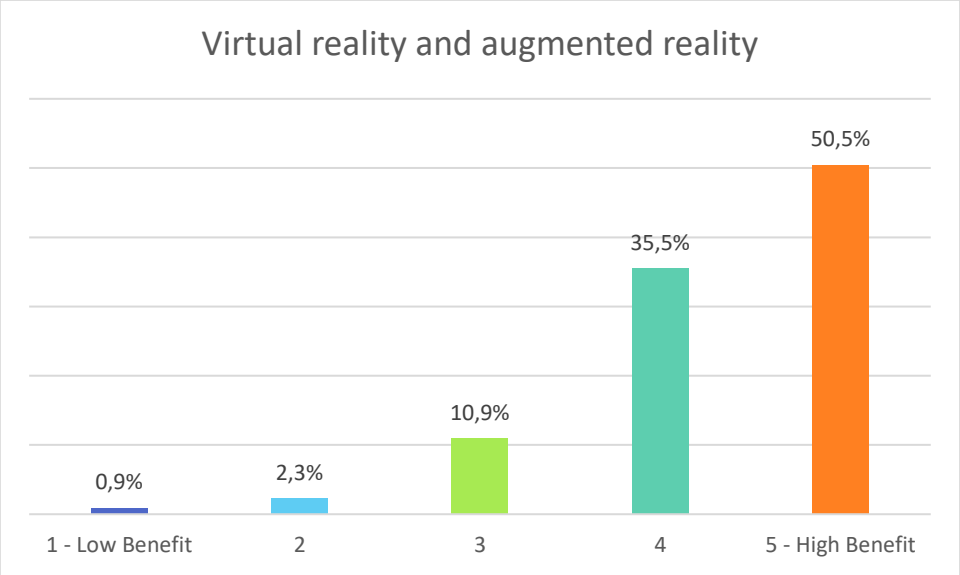
Cloud computing	**Responses (%)**
1 - Low Benefit	0.5%
2	1.4%
3	11.4%
4	33.6%
5 - High Benefit	53.2%

Blockchain



Blockchain	Responses (%)
1 - Low Benefit	0.5%
2	5.0%
3	13.6%
4	40.5%
5 - High Benefit	40.5%

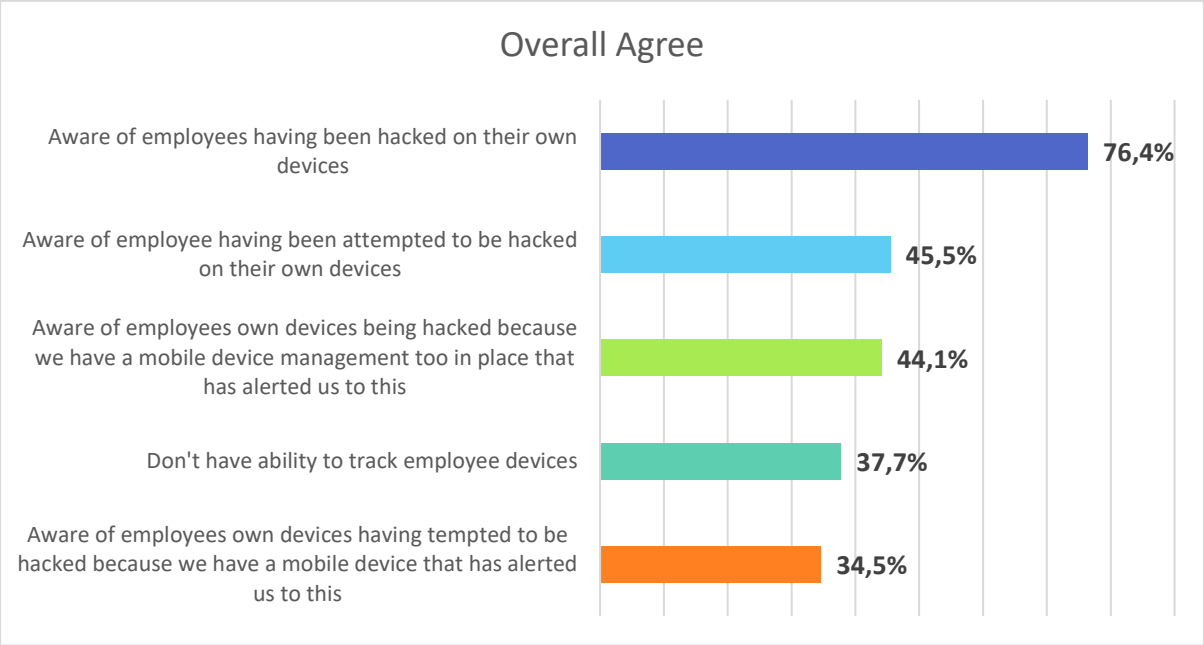
Virtual reality and augmented reality



Virtual reality and augmented reality	**Responses (%)**
1 - Low Benefit	0.9%
2	2.3%
3	10.9%
4	35.5%
5 - High Benefit	50.5%

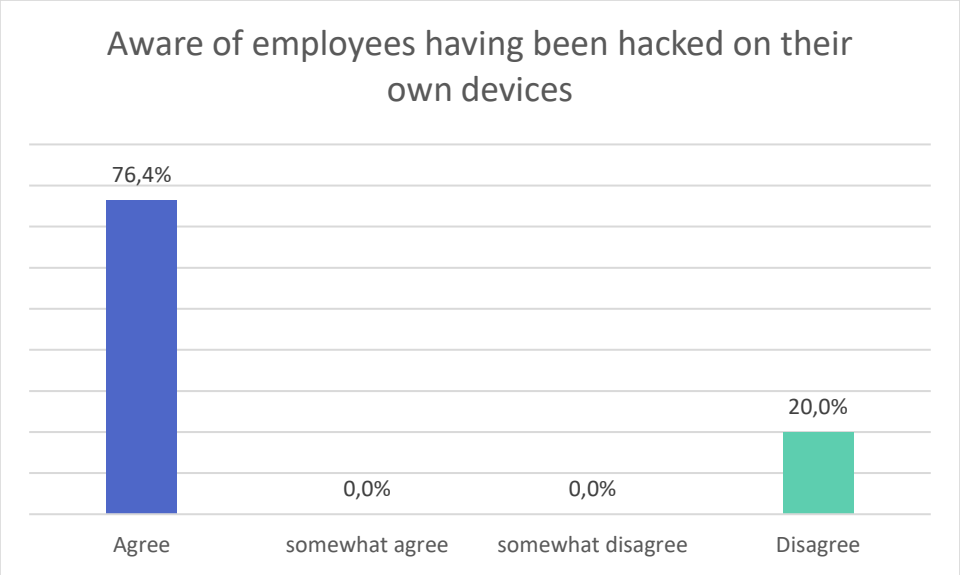
Employee device security

Agree with the following statements



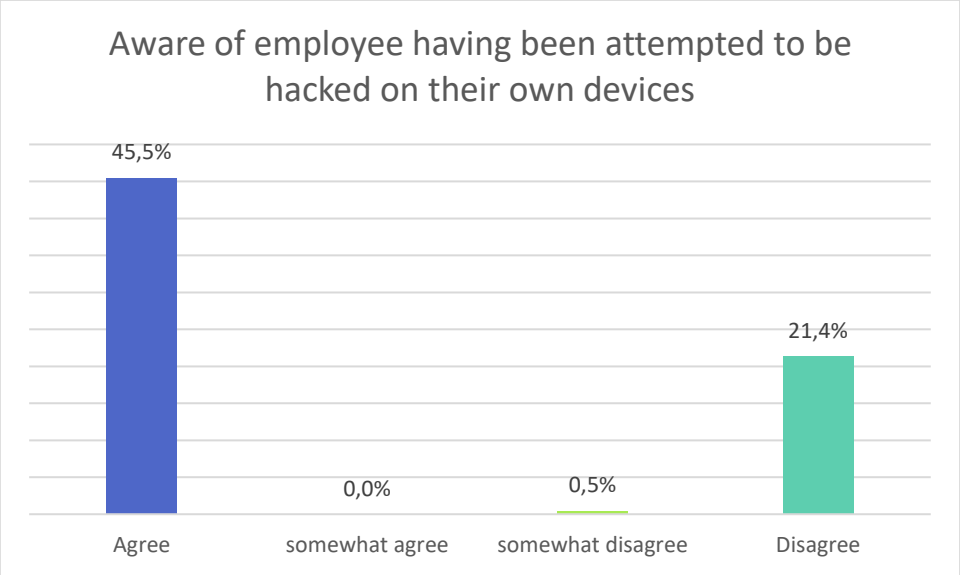
Overall Agree	Responses (%)
Aware of employees having been hacked on their own devices	76.4%
Aware of employee having been attempted to be hacked on their own devices	45.5%
Aware of employees own devices being hacked because we have a mobile device management too in place that has alerted us to this	44.1%
Don't have ability to track employee devices	37.7%
Aware of employees own devices having tempted to be hacked because we have a mobile device that has alerted us to this	34.5%

Aware of employees having been hacked on their own devices



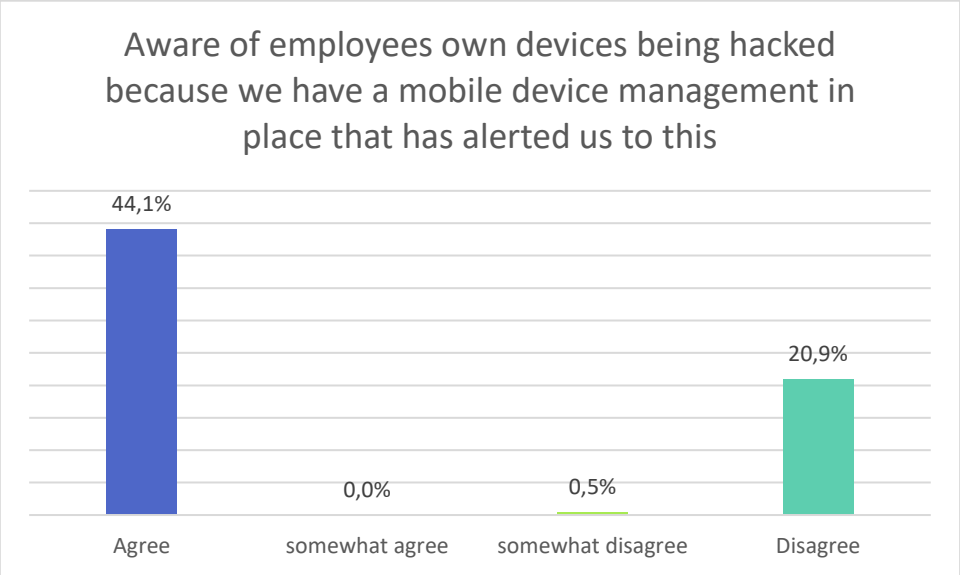
Aware of employees having been hacked on their own devices	**Responses (%)**
Agree	76.4%
Somewhat Agree	0.0%
Somewhat Disagree	0.0%
Disagree	20.0%

Aware of employee having been attempted to be hacked on their own devices



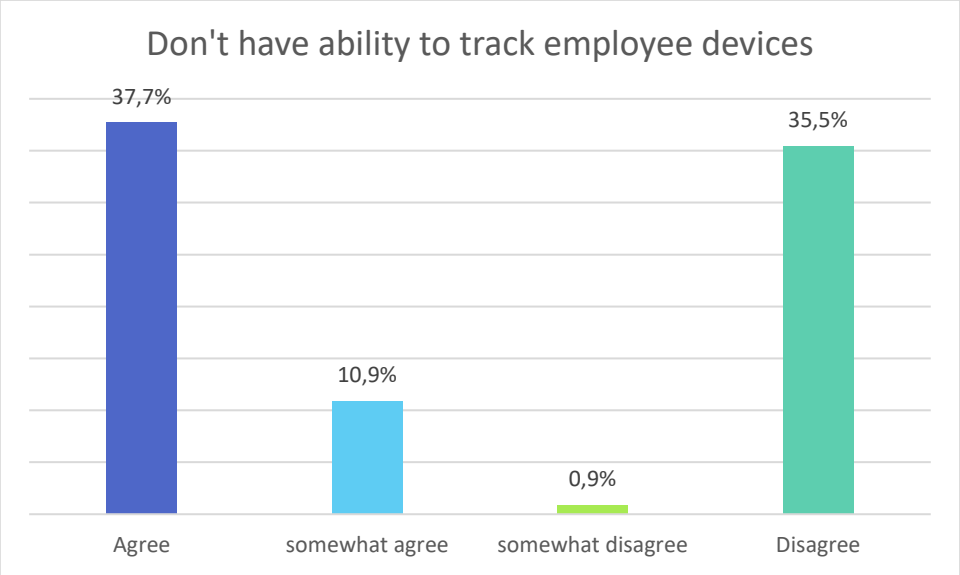
Aware of employee having been attempted to be hacked on their own devices	**Responses (%)**
Agree	45.5%
Somewhat Agree	0.0%
Somewhat Disagree	0.5%
Disagree	21.4%

Aware of employees own devices being hacked because we have a mobile device management in place that has alerted us to this



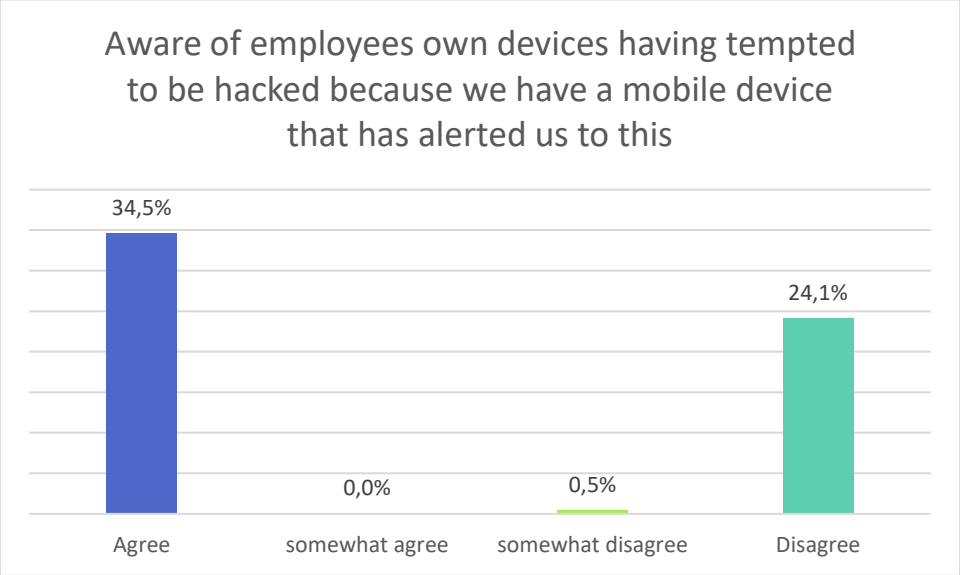
Aware of employees own devices being hacked because we have a mobile device management in place that has alerted us to this	**Responses (%)**
Agree	44.1%
Somewhat Agree	0.0%
Somewhat Disagree	0.5%
Disagree	20.9%

Don't have ability to track employee devices



Don't have ability to track employee devices	Responses (%)
Agree	44.1%
Somewhat Agree	0.0%
Somewhat Disagree	0.5%
Disagree	20.9%

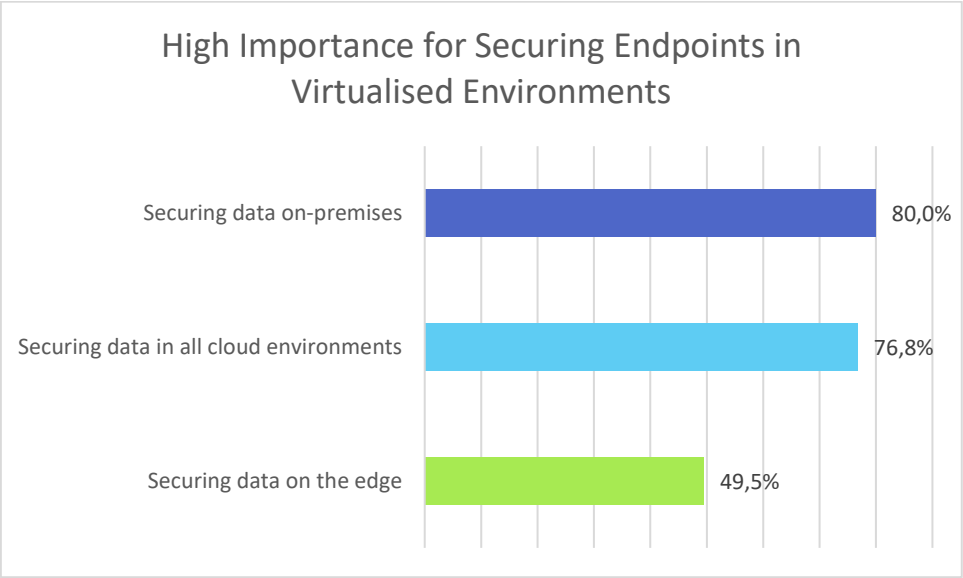
Aware of employees own devices having tempted to be hacked because we have a mobile device that has alerted us to this



Aware of employees own devices having tempted to be hacked because we have a mobile device that has alerted us to this	**Responses (%)**
Agree	34.5%
Somewhat Agree	0.0%
Somewhat Disagree	0.5%
Disagree	24.1%

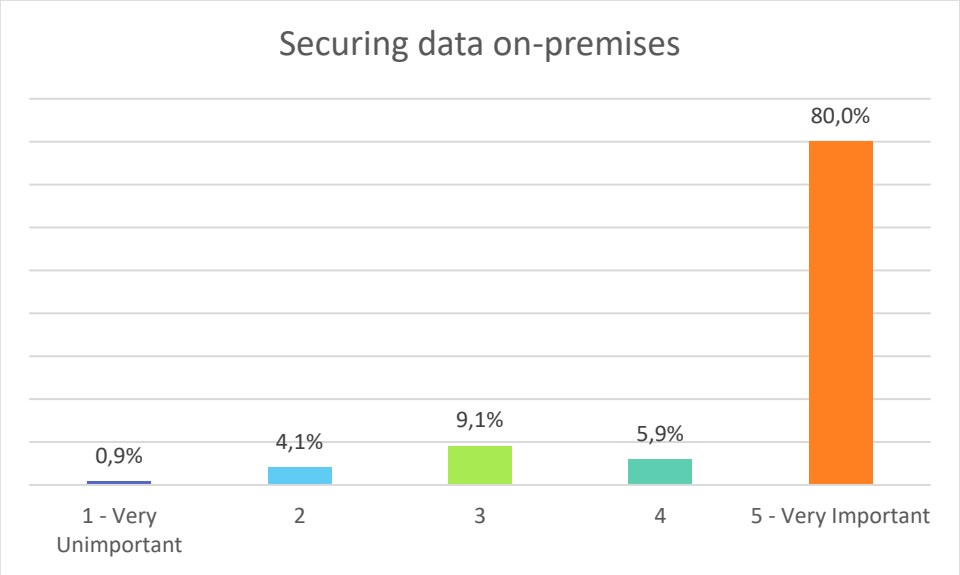
How important are the following when securing endpoints in your virtualised environments?

High Importance



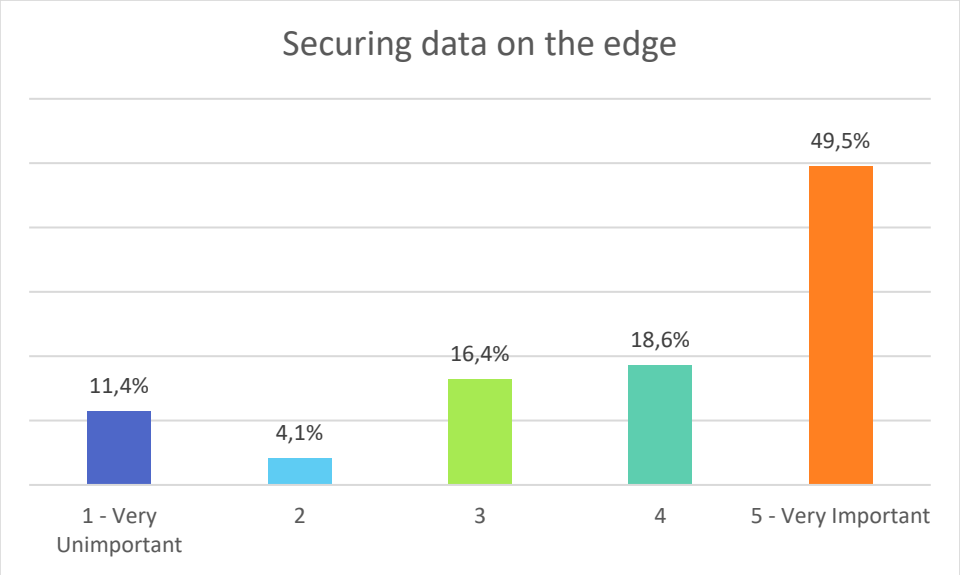
High Importance	Responses (%)
Securing data on-premises	80.0%
Securing data in all cloud environments	76.8%
Securing data on the edge	49.5%

Securing data on-premises



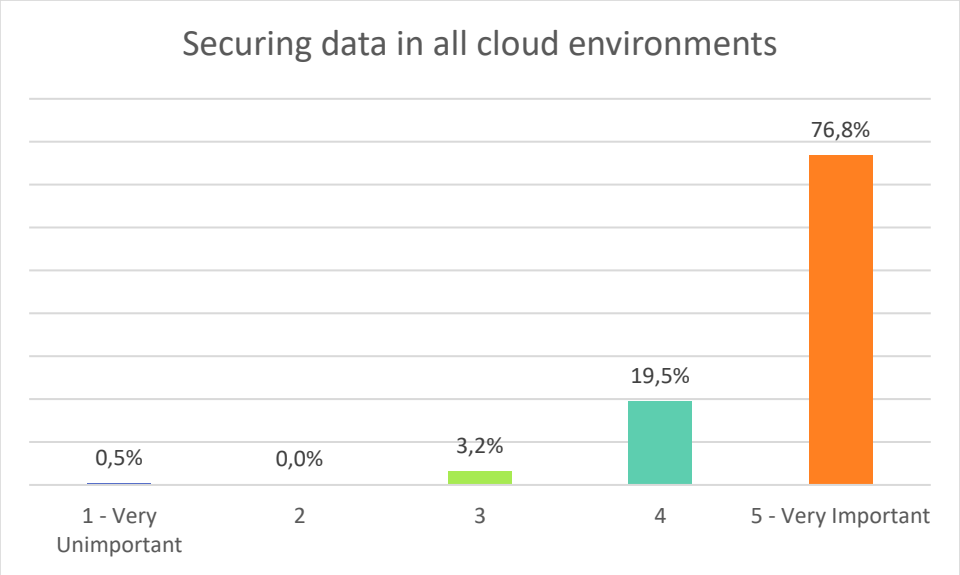
Securing data on-premises	Responses (%)
1 - Very Unimportant	0.9%
2	4.1%
3	9.1%
4	5.9%
5 - Very Important	80.0%

Securing data on the edge



Securing data on the edge	Responses (%)
1 - Very Unimportant	11.4%
2	4.1%
3	16.4%
4	18.6%
5 - Very Important	49.5%

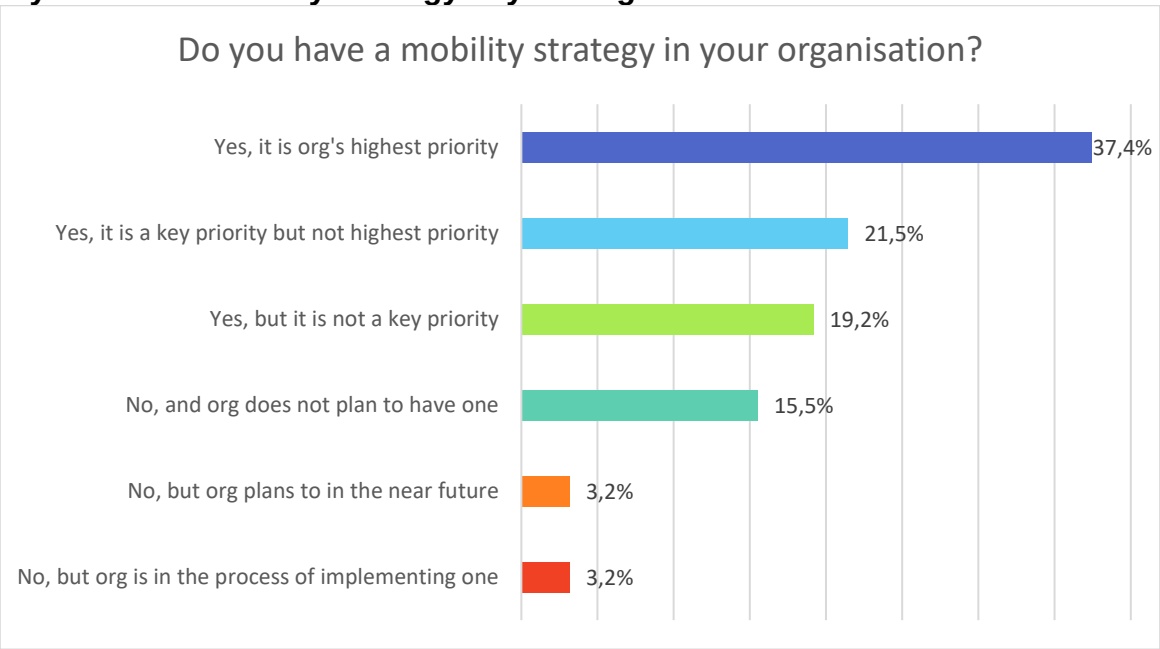
Securing data in all cloud environments



Securing data in all cloud environments	Responses (%)
1 - Very Unimportant	0.5%
2	0.0%
3	3.2%
4	19.5%
5 - Very Important	76.8%

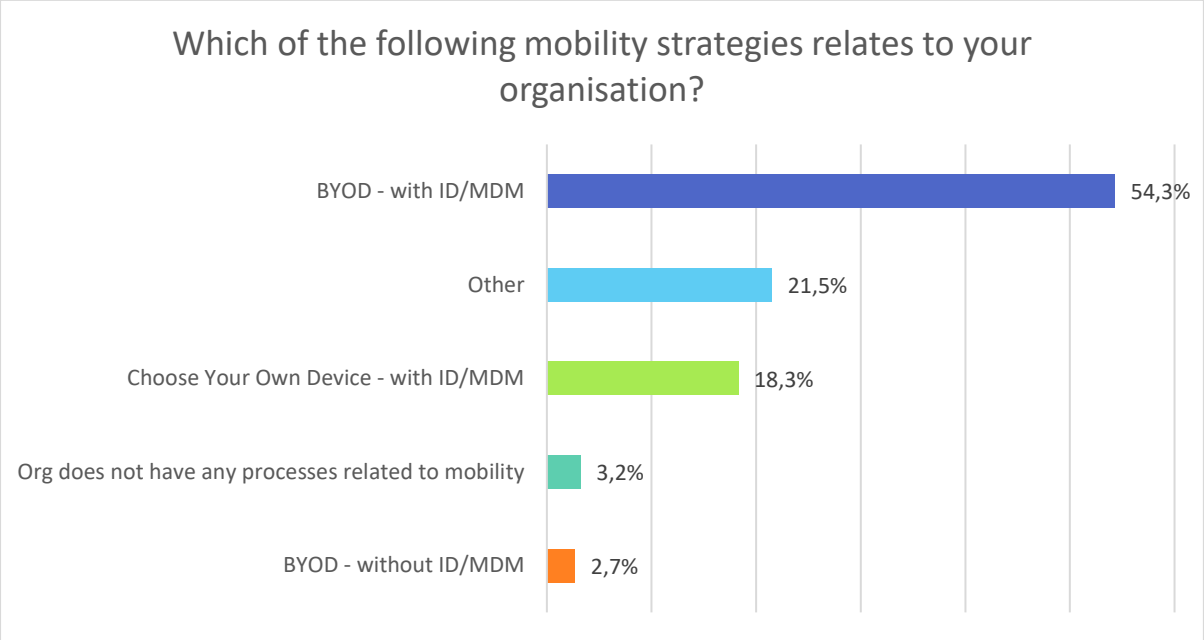
Mobility

Do you have a mobility strategy in your organisation?



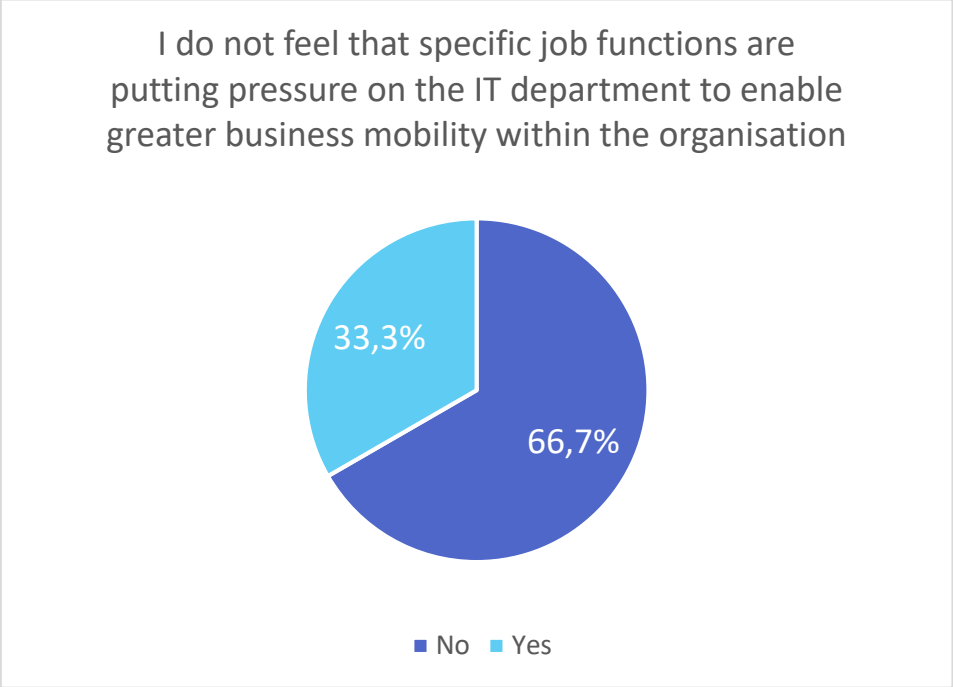
Do you have a mobility strategy in your organisation?	Responses (%)
Yes, it is org's highest priority	37.4%
Yes, it is a key priority but not highest priority	21.5%
Yes, but it is not a key priority	19.2%
No, and org does not plan to have one	15.5%
No, but org plans to in the near future	3.2%
No, but org is in the process of implementing one	3.2%

Which of the following mobility strategies relates to your organisation?



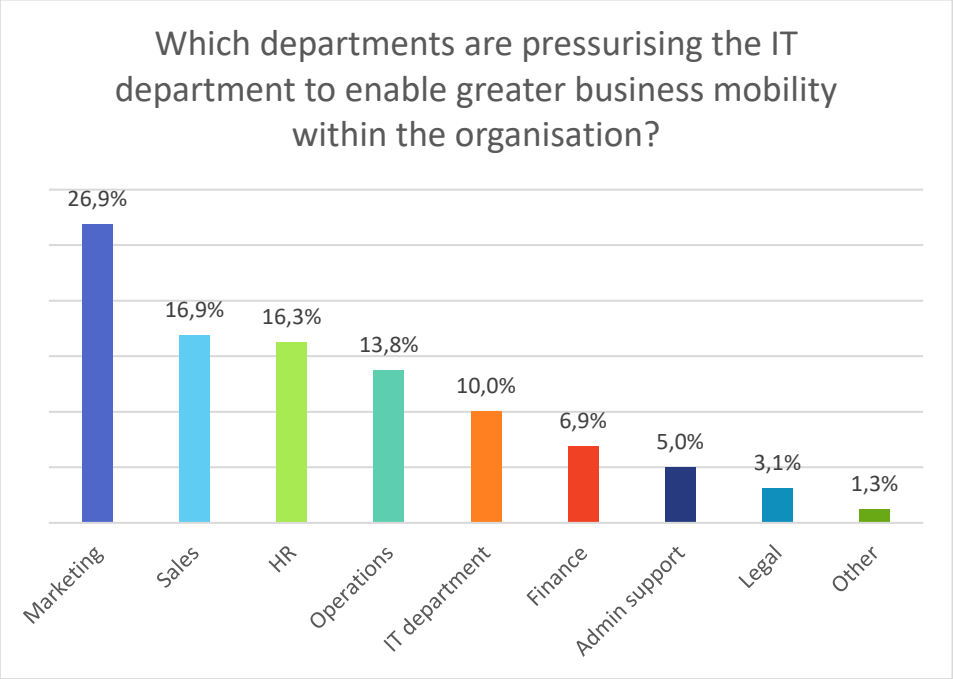
Which of the following mobility strategies relates to your organisation?	Responses (%)
BYOD - with ID/MDM	54.3%
Other	21.5%
Choose Your Own Device - with ID/MDM	18.3%
Org does not have any processes related to mobility	3.2%
BYOD - without ID/MDM	2.7%

I do not feel that specific job functions are putting pressure on the IT department to enable greater business mobility within the organisation



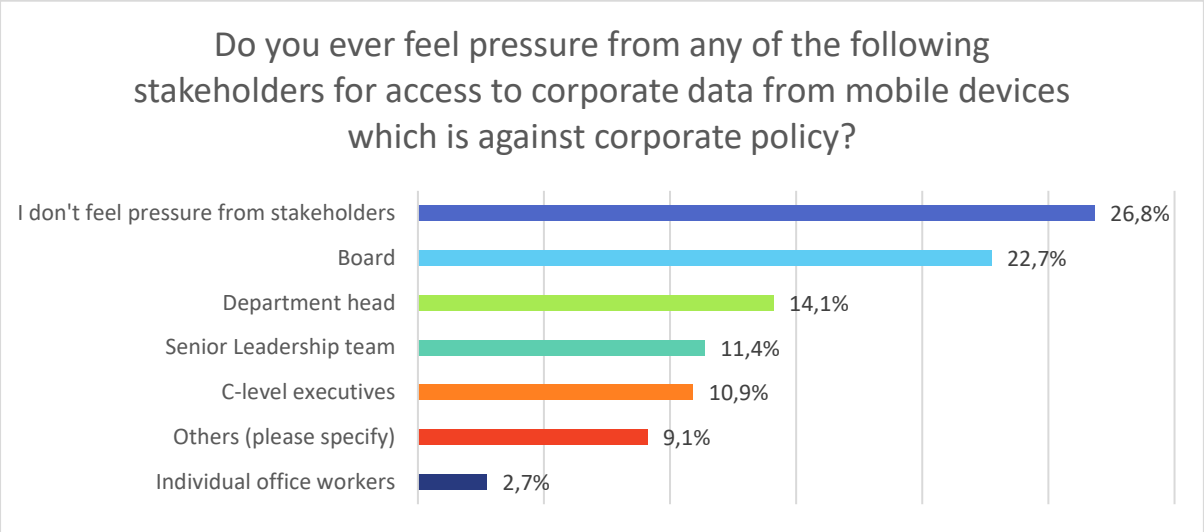
I do not feel that specific job functions are putting pressure on the IT department to enable greater business mobility within the organisation	Responses (%)
No	66.7%
Yes	33.3%

Which departments are pressurising the IT department to enable greater business mobility within the organisation?



Which departments are pressurising the IT department to enable greater business mobility within the organisation?	Responses (%)
Marketing	26.9%
Sales	16.9%
HR	16.3%
Operations	13.8%
IT department	10.0%
Finance	6.9%
Admin support	5.0%
Legal	3.1%
Other	1.3%

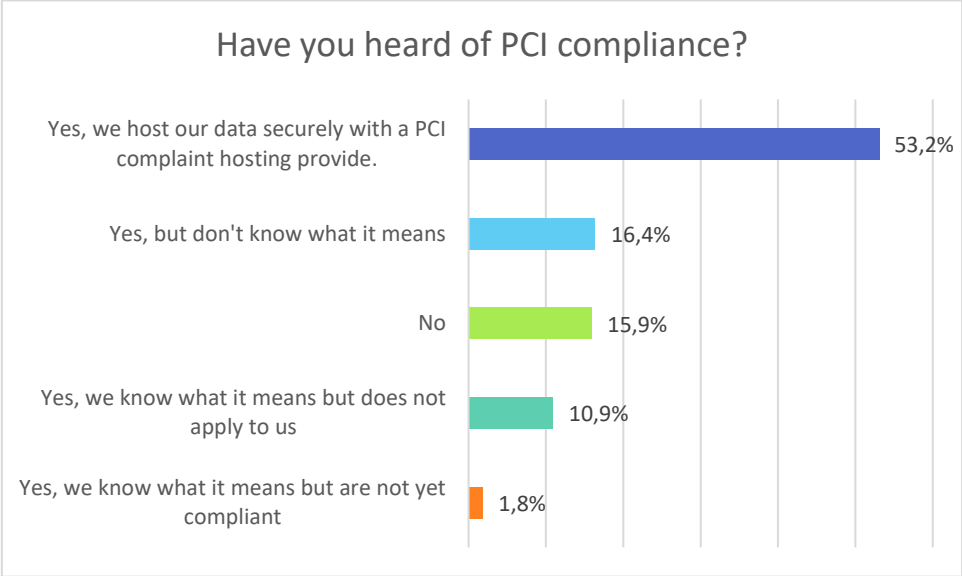
Do you ever feel pressure from any of the following stakeholders for access to corporate data from mobile devices, which is against corporate policy?



Do you ever feel pressure from any of the following stakeholders for access to corporate data from mobile devices, which is against corporate policy?	Responses (%)
I don't feel pressure from stakeholders	26.8%
Board	22.7%
Department head	14.1%
Senior Leadership team	11.4%
C-level executives	10.9%
Others (please specify)	9.1%
Individual office workers	2.7%

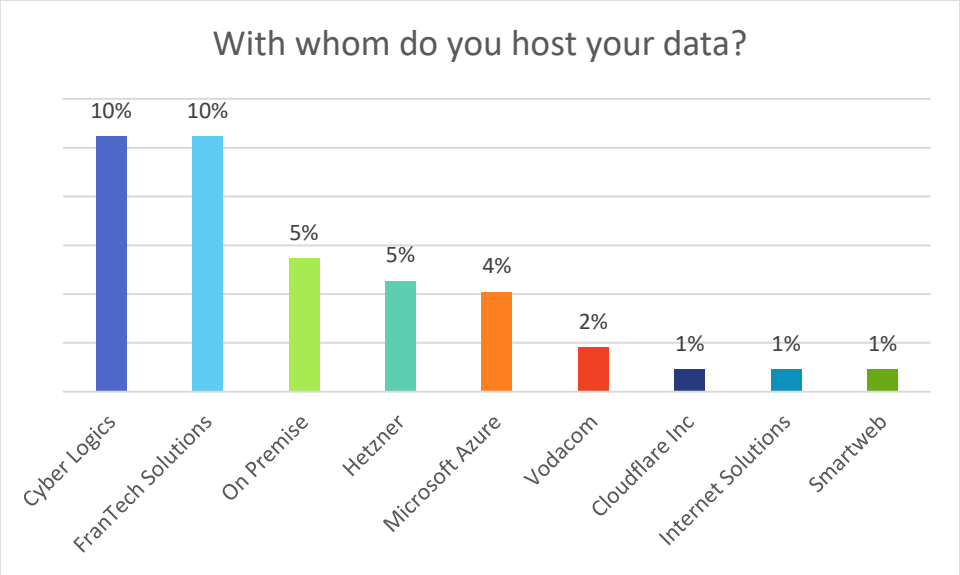
Compliance

PCI (Payment Card Industry) standard compliance



Have you heard of PCI compliance (Payment Card Industry data security standard)?	Responses (%)
Yes, we host our data securely with a PCI complaint hosting provide.	53.2%
Yes, but don't know what it means	16.4%
No	15.9%
Yes, we know what it means but does not apply to us	10.9%
Yes, we know what it means but are not yet compliant	1.8%

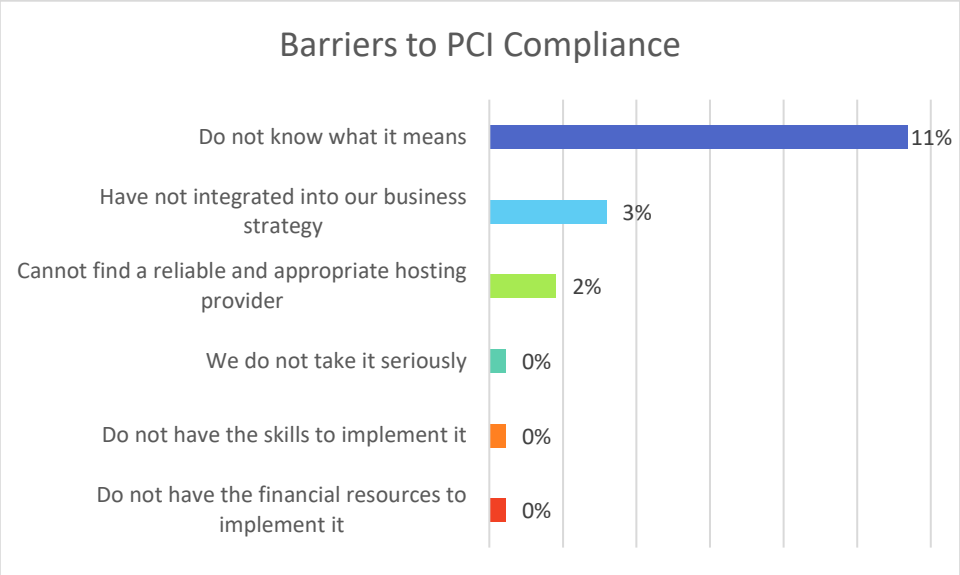
If yes to the above, with whom do you host your data?



While there are 30 different distinct providers, the top providers are Cyber Logics, FranTech Solutions, and hosting on-premise.

If yes above, with whom do you host your data?	**Responses (%)**
Cyber Logics	10%
FranTech Solutions	10%
On Premise	5%
Hetzner	5%
Microsoft Azure	4%
Vodacom	2%
Cloudflare Inc	1%
Internet Solutions	1%
Smartweb	1%

If no to the above, what are the barriers to PCI compliance?



If no was selected, what are the barriers to PCI compliance?	**Responses (%)**
Do not know what it means	11%
Have not integrated into our business strategy	3%
Cannot find a reliable and appropriate hosting provider	2%
We do not take it seriously	0%
Do not have the skills to implement it	0%
Do not have the financial resources to implement it	0%