Cybercrime Survey 2021

62 %

expects its cyber and information security budget to grow within the next 12 months.

78 %

states that organised criminals constitute the greatest threat in relation to cyber and information security.

81 %

of CXOs are concerned that critical systems will become inaccessible for a long period of time, which is a record-breaking number.

Audit. Tax. Consulting.

pwc

Together we succeed ...

402 business executives, IT managers and specialists from Danish organisations participated in PwC's Cybercrime Survey 2021, sharing their views on various developments and challenges in relation to cybercrime in Denmark.

They have thus assessed the threat landscape and reported how and to what extent they are dealing with the challenges.

Contents

Record-breaking level of concern about organised cyber criminals

The Cybercrime Survey 2021 shows that organised criminals now pose the greatest threat in relation to cyber and information security. As many as 78 % of respondents consider organised criminals to be among the greatest cyber threats, which is the highest number in the history of the Cybercrime Survey (since 2015). Likewise, the Centre for Cyber Security estimates that the cybercrime threat is ‘very serious’ in Denmark, just as it has found cyber criminals to be developing their skills and launching new types of attack.[1] This applies, for example, to the criminals behind ransomware attacks, who are increasingly using advanced types of attack. Criminal hackers not only carry out ‘classic’ ransomware attacks involving encryption of organisations’ data, they are also stealing data enabling them to further threaten organisations and individuals with leaking the stolen, sensitive information unless a ransom is paid.

Advanced cyber attacks you would want to avoid

Recent years have shown some of the most advanced attacks in history. In 2020, an IT security company in the US was subjected to a supply chain attacks in which cyber criminals implemented malicious code (malware) in an update to a customer-facing software system. This allowed the hackers to spy on a wide range of organisations in critical social sectors, leaving the companies running the software update vulnerable. In 2021, another advanced attack took place. The target was yet again a large organisation where a group of hackers exploited a security gap in a customer-facing e-mail system. The organisation was not aware of the security gap before the attack – a genuine so-called zero-day vulnerability. This attack also opened a backdoor to sensitive information such as e-mails and calendar information. These new advanced types of attack put the business sector and society alike under pressure when thousands, if not millions, of businesses become vulnerable at the same time. PwC has also learnt that a significantly higher number of organisations are concerned about coming under such an attack. This is supported by the fact that, on several occasions, PwC’s incident response team has had to establish actual incident response processes to be able to contact more than 1,000 vulnerable Danish organisations in a very short time.

In the past, we have seen how media coverage of cyber incidents or personally experienced attacks have resulted in greater cybersecurity investments because organisations have become aware of the fatal consequences of such attacks, for example reputational damage or financial losses. Today, we see that organisations to a greater extent invest in security measures on their own initiative before an attack has taken place. Moreover, PwC has learnt that more and more organisations – to mitigate the cyber threat – are investing in multi-year transformation security programmes and establishing security technologies which genuinely safeguard the organisation’s critical assets.

Sharper focus on cybersecurity by top management

A focussed and prioritised effort is required by Management to enable an organisation to implement the right, effective security measures. Consequently, it is a positive sign that in the assessment of as many as 8 out of 10 (80%) of the respondents, the executive board/Management is focussed on achieving the right balance between cyber threats and investments in cybersecurity.

At the same time, however, we see room for improvement when it comes to communication and/or security reporting across management levels from the security department to the executive board and the board of directors. The lack of communication impedes a clear and adequate understanding of the security issues by Management, risking that the required efforts will not be given proper priority.

As a consequence, when working on the cyber strategy, it is crucial that top management and the board of directors implement a regular practice for reporting and communicating about the current threat picture, incidents, prioritised measures, etc. This facilitates the development of a holistic cyber strategy, which includes reliable internal and external security management. You see, cybersecurity is, among other things, about building trust and showing the outside world that it may safely do business and enter into relationships with the organisation. Such trust is an asset to be protected by the organisation.

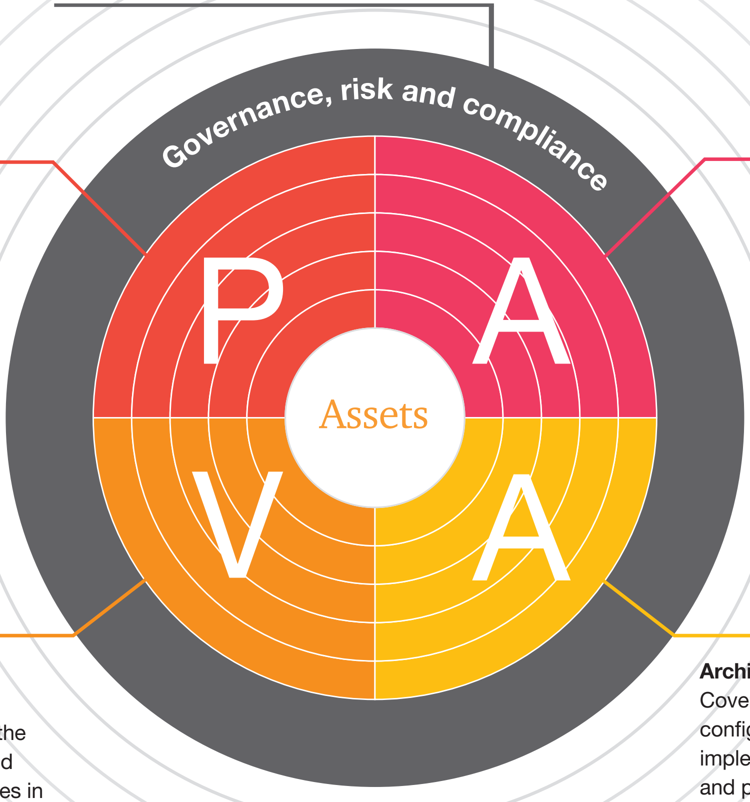
Mads
Nørgaard Madsen
Partner
Technology & Security

[1] https://cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/

PAVA – a comprehensible security concept

Once again, this year's survey results are structured on the basis of PwC's PAVA concept. In our experience, this concept may contribute to a common understanding between top management and the security professionals. The PAVA concept is a generic communication, assessment and reporting concept that organisations use to assess their maturity level and resilience to different types of cyber risks and threats. The concept can be applied across a variety of security standards and frameworks and therefore accommodate such complexity, while providing clear focus areas for comparison with other organisations. In this way, PAVA provides a common basis for concrete and priority solutions in specific security areas within the organisation for use in a wider context and for continuous impact assessment. PAVA covers five main areas – from governance, risk and compliance to process, behaviour, validation and architecture. Depending on the level of maturity and security of each organisation, there is a need for action in all areas, to achieve long-term and stable cyber and information security. This structure also follows most organisations' way of distributing responsibilities and roles for security work, and it is possible to focus on individual areas according to need without losing focus.

Governance, risk and compliance area
The framework that the organisation has or should put in place to ensure a risk managed prioritisation of security measures as well as to comply with applicable laws and regulations.



Process area
Covers the processes and procedures which will contribute to a standardised approach to security.

Behavioural area
Includes the employees' awareness and competence levels in terms of protecting the organisation's information and assets.

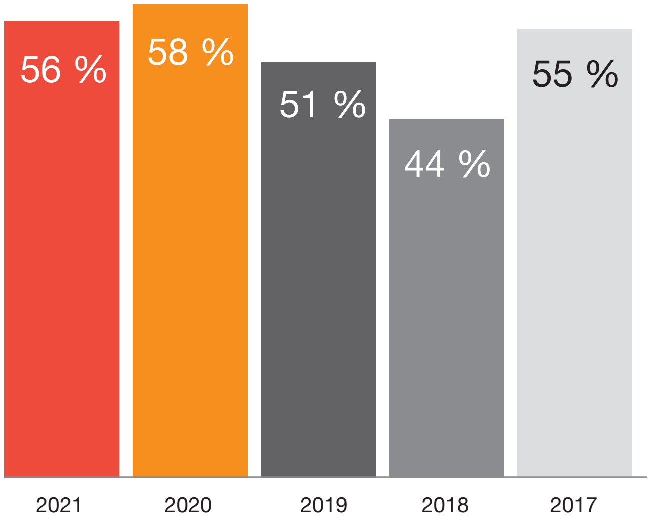
Validation area
Describes the activities which will contribute to the continuous detection and verification of weaknesses in the organisation's technical and organisational controls.

Architecture area
Covers the design, configuration and implementation of technical and physical solutions for the protection of the organisation's assets.

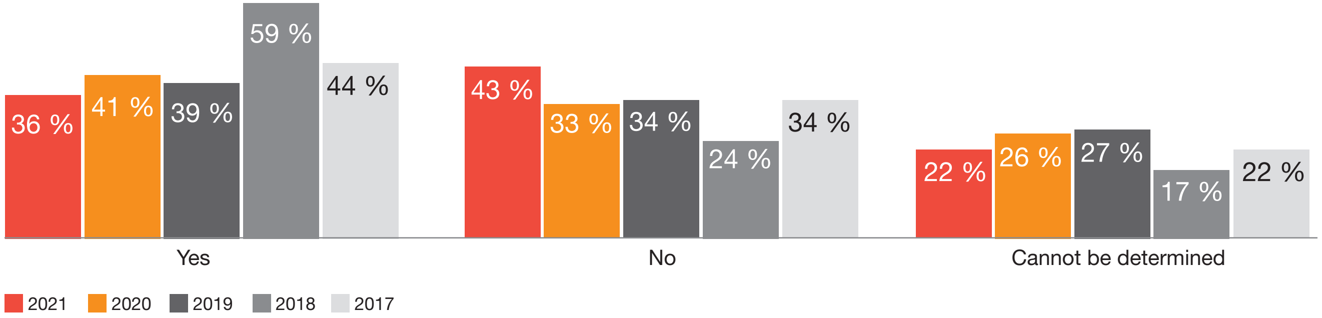
Every other organisation has experienced at least one security incident

More than half (56 %) of the respondents in the Cybercrime Survey 2021 state that their organisation has experienced at least one security incident within the past financial year. This is roughly on a par with 2020 (58%). Moreover, the survey shows that, in 2021, more than every third (36%) has experienced one or more security incidents targeting their organisation, which is a small decline compared to 2020 (41%). Organisations remain concerned about the cyber threat and, in 2021, more than half of respondents (54%) state that they are more concerned about the cyber threat today than 12 months ago.

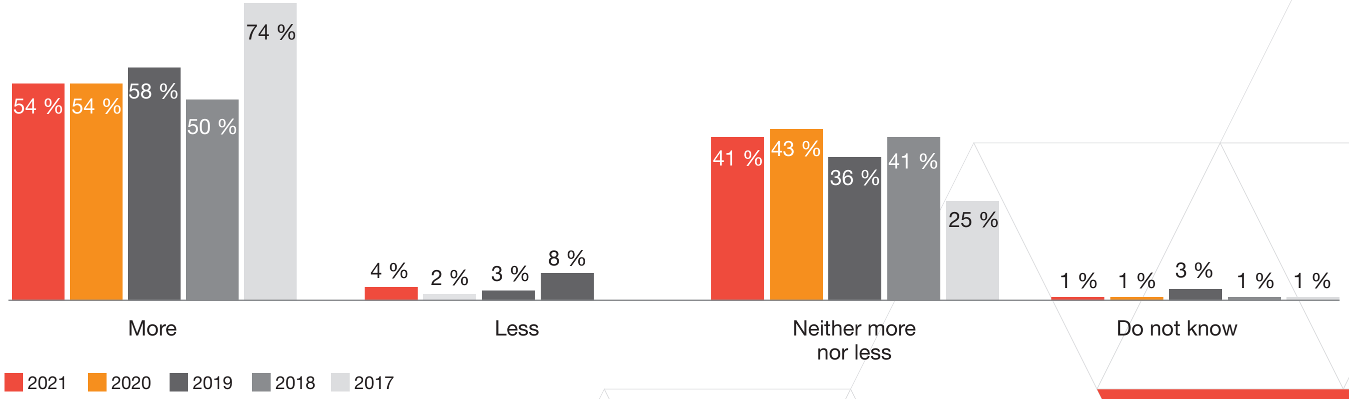
Have experienced at least one incident



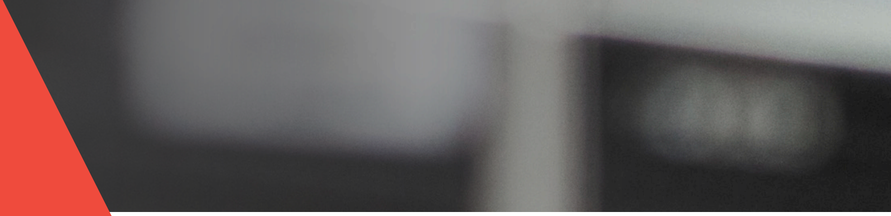
Has your organisation experienced one or more security incidents targeted at your organisation?



Do you worry more or less about the cyber threats that your organisation is confronted with today compared to 12 months ago?



Continued high degree of confidence in the financial sector's data and cybersecurity



It is important to the level of trust in society that each citizen feels confident that the public and private sectors manage data securely and in accordance with applicable legal requirements and rules.

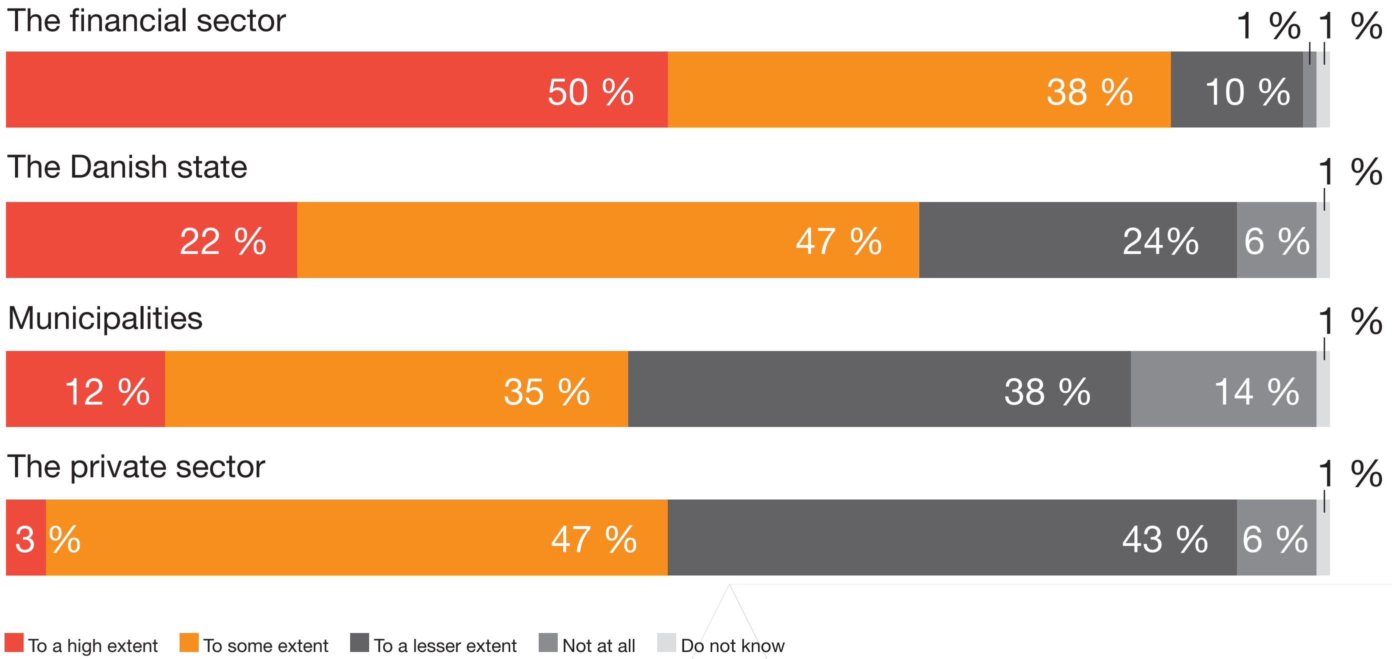
Looking across sectors at the level of confidence in GDPR compliance, the Cybercrime Survey 2021 shows the financial sector remaining at the top. Almost 9 out of 10 (88 %) of respondents state that to some or a high extent they have confidence in the level of GDPR compliance in the financial sector, which is on a par with last year.

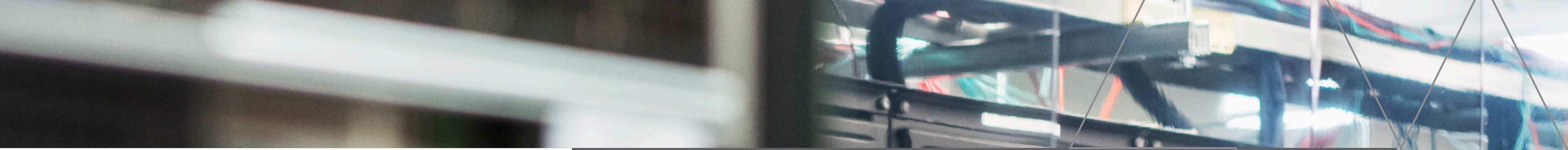
Approx. 7 out of 10 (69 %) indicate to have some or a high degree of confidence in the Danish state's GDPR compliance management, which is an increase on 2020 (64 %).

Looking at the confidence in the GDPR compliance of municipalities, the potential for improvement remains considerable. In 2021, 47 % indicates that to some or a high extent they have confidence in the GDPR compliance level of municipalities, which is a small increase compared to 2020 (42 %). However, it is worth mentioning that as many as 38 % indicated to have little confidence in the GDPR compliance of the municipalities, and that 14 % has no confidence in the GDPR compliance management of this sector.

In the private sector, there is also room for improvement with 50 % indicating that they have confidence in this sector's GDPR management to some or a high extent, while as many as 43 % replied 'to a lesser extent'.

To what extent do you have confidence in the GDPR compliance level of the sectors below?

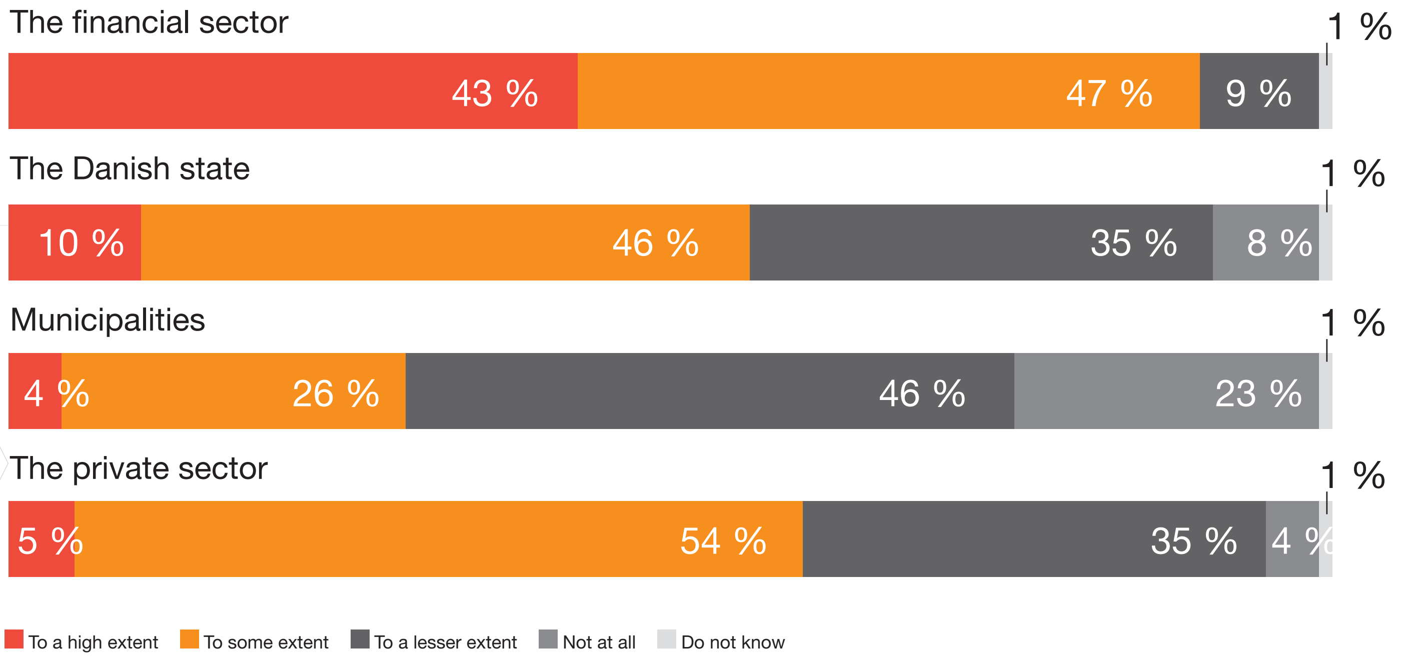


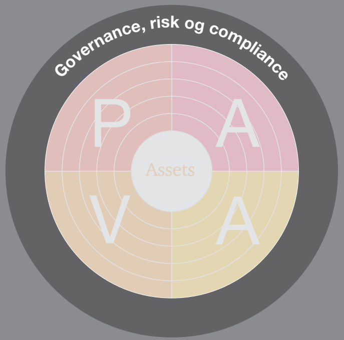


In terms of cybersecurity confidence, the picture remains broadly unchanged across sectors compared to 2020. The level of confidence in the financial sector's cybersecurity remains the highest with as many as 90 % of respondents reporting to have some or a high degree of confidence in the financial sector's cybersecurity measures (89 % in 2020). Confidence in cybersecurity measures of the municipalities remain the lowest. Only 30 % reports to have some or a high degree of confidence in the cybersecurity measures of the municipalities (31 % in 2020).

PwC recommends: Trust is essential to people, organisations and enterprises in developing and creating relationships. All other things being equal, an organisation or enterprise which inspires trust will do better in terms of creating relationships with customers, employees and the external environment than an organisation or enterprise which does not. Cybersecurity may contribute to building trust in the organisation's management of data. PwC therefore recommends that organisations ensure correct and secure data management.

To what extent do you have confidence in the cybersecurity measures of the sectors below?





PAVA

Governance, risk and compliance

Game of Threats™

PwC's Game of Threats is especially designed to provide the management with interactive training in the risks associated with cybercrime and the importance of investing in cyber and information security.

Read more at www.pwc.dk/cyberaware

Board of Directors

The Cybercrime Survey 2021 shows that only 15% of the board members participating in the survey indicate that the mix of competencies of the board to a high extent ensures deep enough knowledge of cyber and information security. In addition, 61% reports that the Board of Directors does not receive cyber and information security training. This is nonetheless a significant improvement from 2020 when as many as 89 % of board members indicated that no cyber training or educational programme had been established for the board.

The top management is more concerned about the impact of cyber incidents

Cybersecurity requires top management's understanding and prioritisation to enable the organisation to implement adequate, effective security measures based on a risk assessment.

This year's survey shows that several CXOs[2] are concerned about the impact of a security incident. The primary concern of CXOs and security professionals[3] this year is that critical systems become inaccessible for a long time. This was also the case in 2020.

This year, as many as 81% of CXOs are concerned that critical systems will become inaccessible for a long period of time, which is an increase of 11 percentage points compared to 2020.

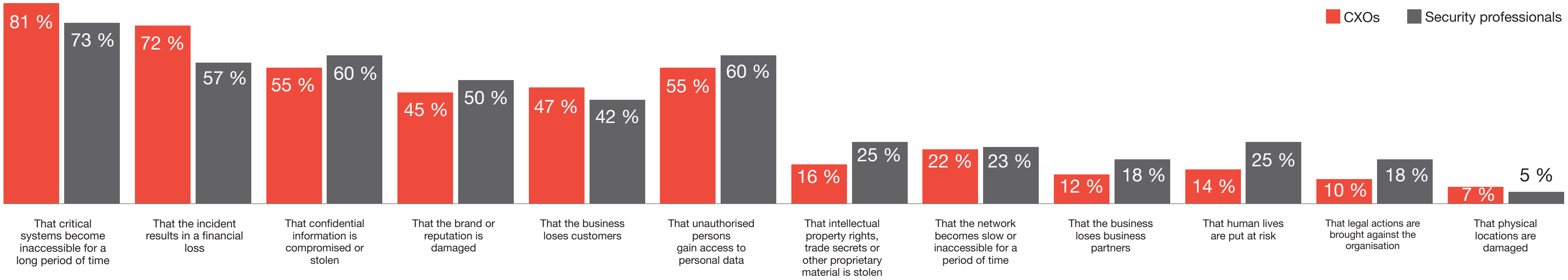
The number of CXOs who are concerned about a security incident resulting in a financial loss, the organisation's confidential information being compromised or stolen, or unauthorised access to personal data has also increased compared to last year. These topics are also top of the list of security professionals' concerns.

[2] Includes the job titles CEO, CFO, CIO, CCO, CTO, etc

[3] Includes the job titles CISO, security officers, security specialists and other employees.

PwC recommends: Management needs to keep focussing on prioritising, motivating and sponsoring the fight against cybercrime to prevent the loss or inaccessibility of the organisation's critical assets for a long period of time. Organisations are still required to plan several years ahead to strengthen cybersecurity.

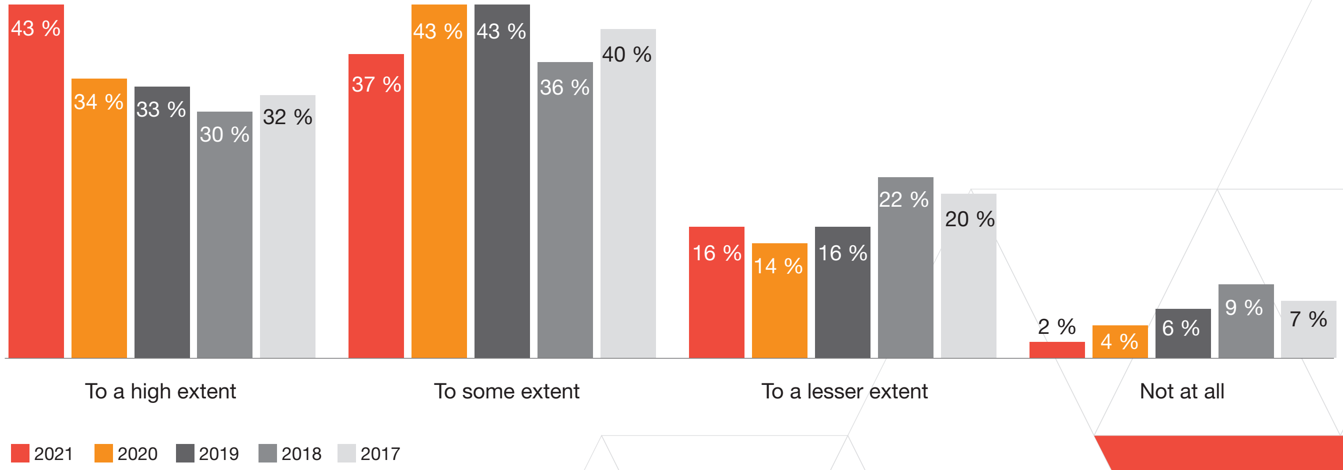
What is your organisation’s main concern regarding the consequences of a cyber incident?



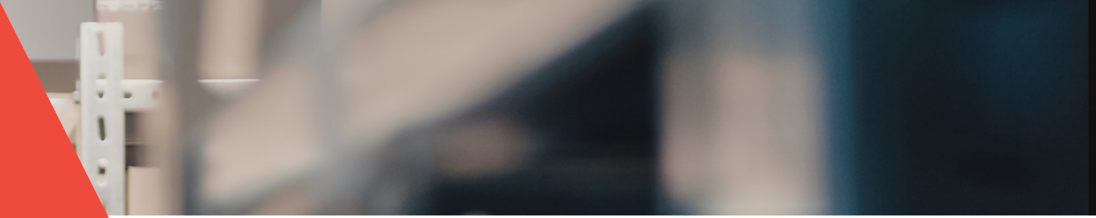
In 2020, one in four (24 %) of respondents believed that the lack of understanding by top management posed a threat to the organisation. The fact that top management this year is more concerned about the impact of cyber incidents may have changed this view. In 2021, only 16 % reports that top management’s lack of understanding poses a threat to the organisation (see the graph on page 18).

This year, 80 % believes that, to some or a high extent, the executive board/top management focusses on striking the right balance between cyber threats and investments in cybersecurity (77 % in 2020). The positive development becomes even more evident when we only look at the proportion who answered ’to a high extent’. Thus, as many as 43 % of respondents assess their management team to be focussed, to a high extent, on striking the right balance, which is an increase of 9 percentage points on 2020.

To what extent is the executive board/management of your organisation, in your opinion, focussed on achieving the right balance between the cyber threats faced by your organisation and investments in cybersecurity?

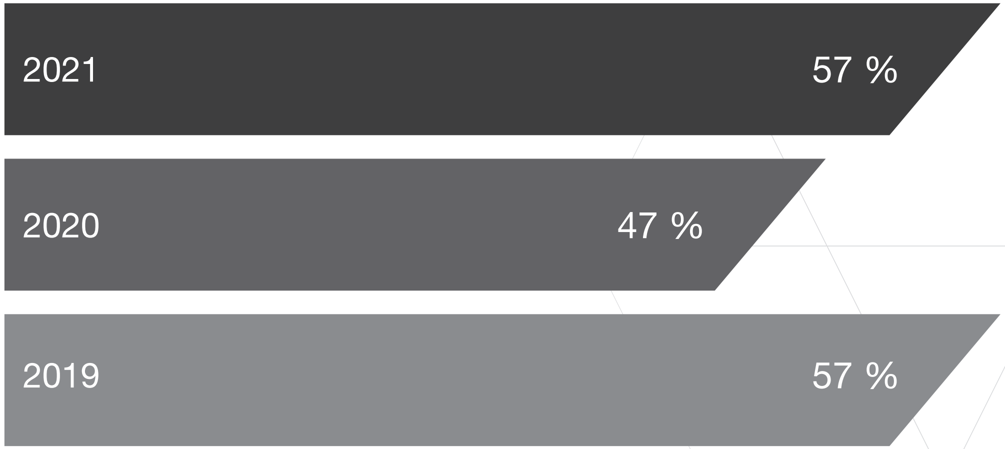


Focus on protection of personal data has increased significantly



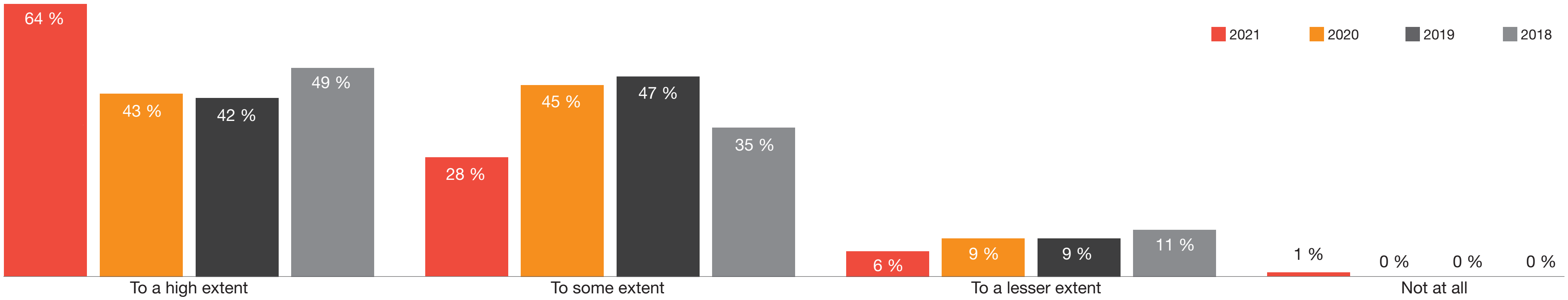
More than half (57 %) of the respondents this year indicate that one of their major concerns in relation to the consequences of a cyber incident is ‘unauthorised access to personal data’. The increase from 47% in 2020 is thus significant.

Percentage stating a concern about unauthorised access to personal data:

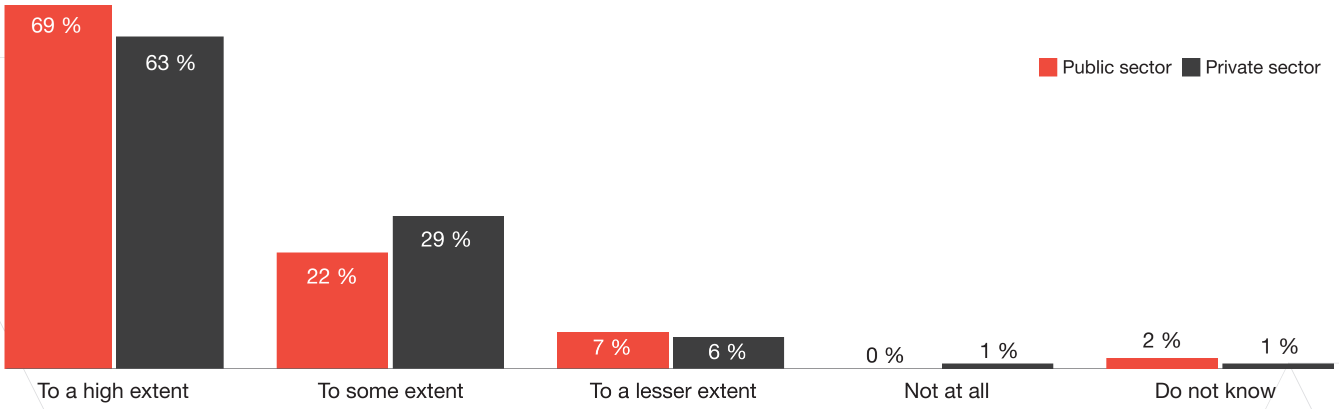


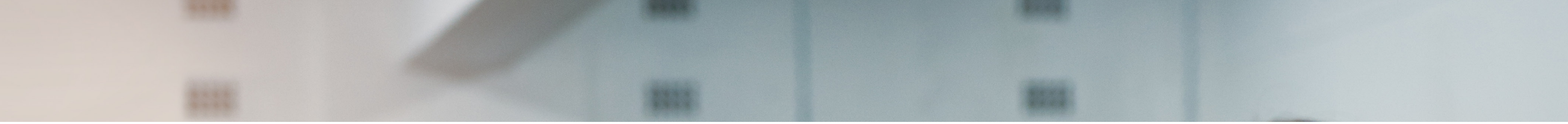
Moreover, we see that organisations are increasingly focussed on protecting personal data in accordance with the GDPR. Accordingly, 9 out of 10 (92 %) respondents report that their organisation's personal data are to some or a high extent adequately protected in accordance with the GDPR. The share answering 'to a high extent' has increased from 43 % in 2020 to a record-breaking 64% this year.

To what extent are your organisation's personal data protected in accordance with the General Data Protection Regulation (GDPR)?



It is the assessment of the public and private sectors alike that personal data are protected in accordance with the GDPR. However, the public sector's assessment of itself is slightly better than that of the private sector. Thus, 69 % of public sector respondents believe that their organisation to a high extent protects personal data in accordance with the GDPR, while this number is 63 % for the private sector.

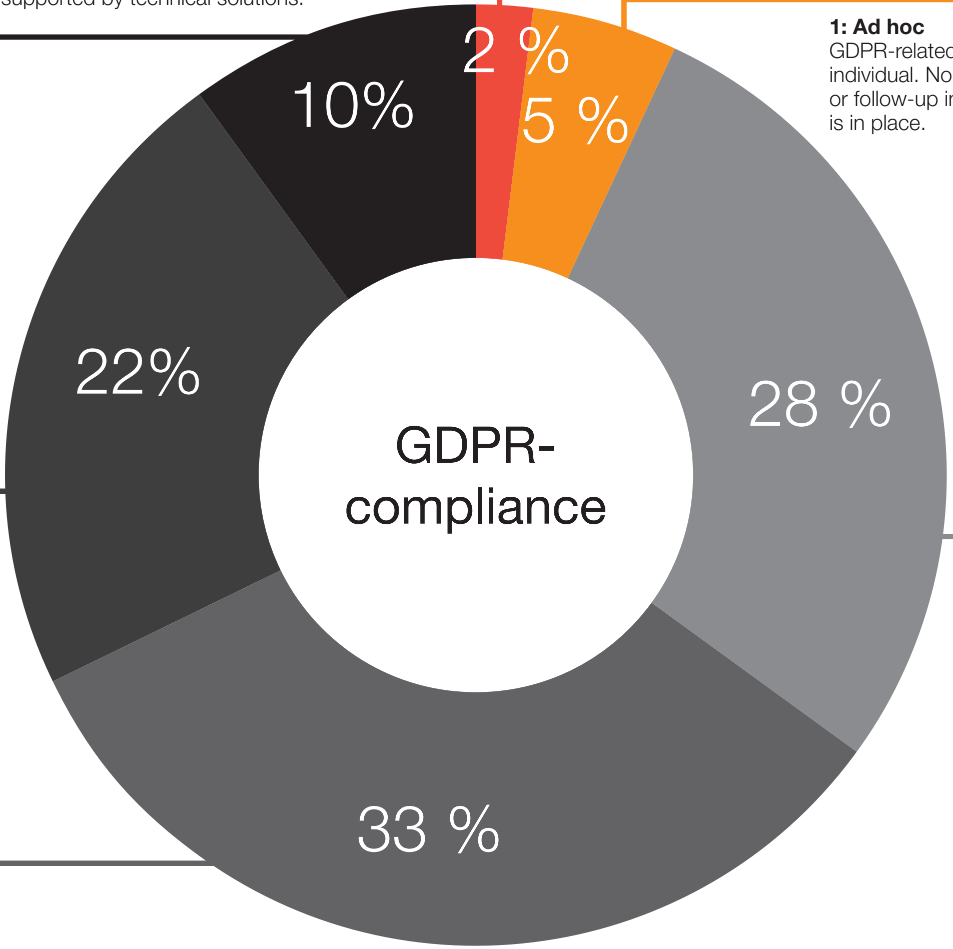




When PwC assists organisations in assessing their level of GDPR compliance, our GDPR experts use a scale of 0 to 5 where 5 is best (see chart).

28 % of respondents indicate that the organisation's GDPR compliance level is reactive (level 2). In positive terms, more than half (55 %) of respondents indicate that their GDPR compliance level is 'Defined' or 'Quantitatively managed' (levels 3 and 4, respectively).

In your opinion, what is the GDPR compliance level of your organisation?



0: Non-existent
No noticeable GDPR-related work is being carried out.

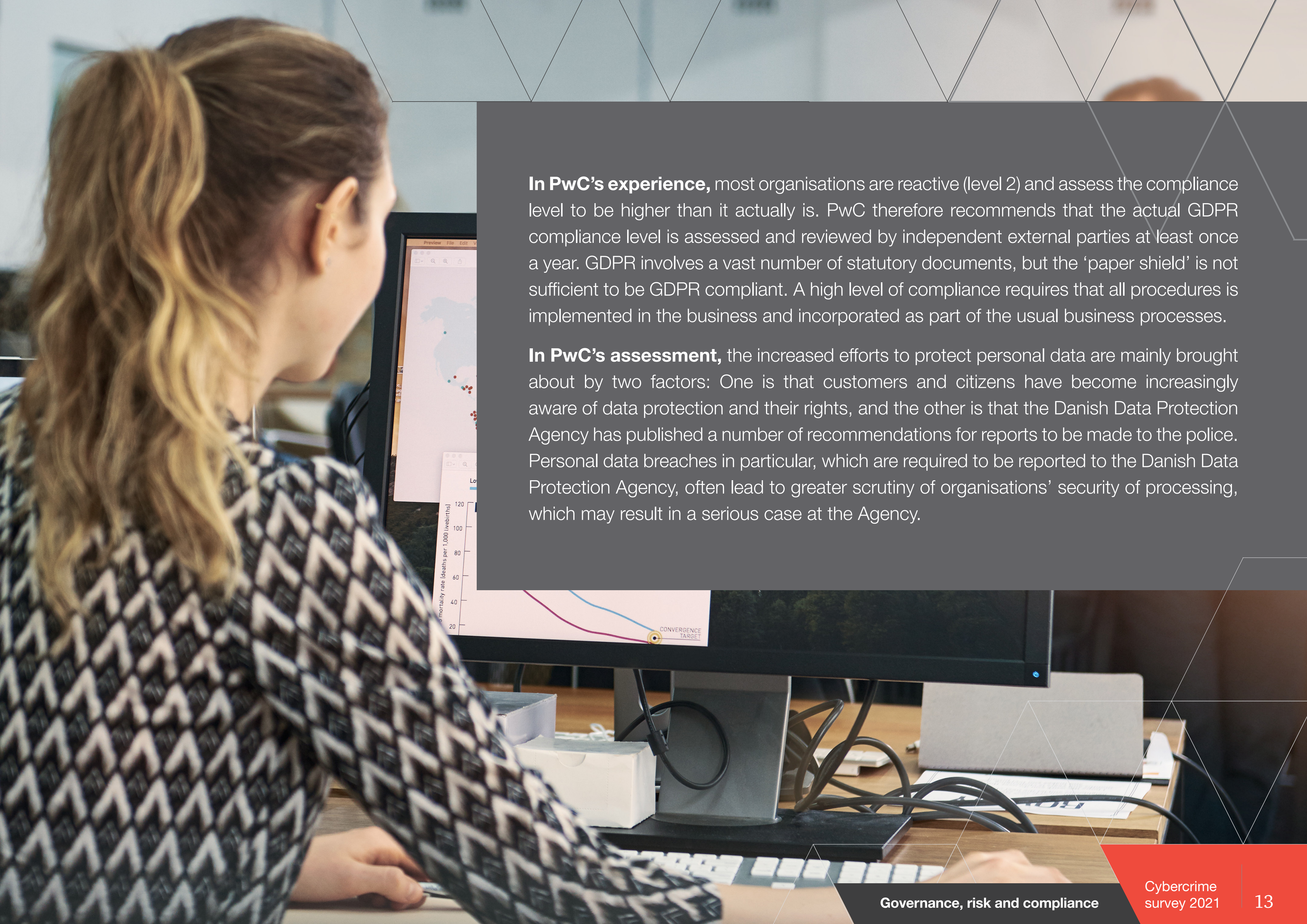
1: Ad hoc
GDPR-related responsibility is left to the individual. No procedures, awareness training or follow-up in relation to GDPR compliance is in place.

2: Reactive
Formalised GDPR management and procedures are in place. A few procedures are in place, and these have been communicated to the organisation, however, they have not been adequately implemented.

3: Defined
Everyone is familiar with their role, responsibilities and tasks. Procedures have been approved by Management, and the entire organisation works in accordance with the procedures. Targeted training is carried out, and sufficient tools have been provided to carry out the tasks.

4: Quantitatively managed
Procedures have been approved by management, and the entire organisation works strictly in accordance with the procedures. Continuous monitoring is in place, including follow-up of activities, and this is reported to Management on a regular basis.

5: Optimised
GDPR is a top priority of management, and the organisation focusses on new effective and efficient methods to improve the compliance level. Assessments of the compliance level are carried out by an external partner on an ongoing basis, and the work is supported by technical solutions.



In PwC's experience, most organisations are reactive (level 2) and assess the compliance level to be higher than it actually is. PwC therefore recommends that the actual GDPR compliance level is assessed and reviewed by independent external parties at least once a year. GDPR involves a vast number of statutory documents, but the 'paper shield' is not sufficient to be GDPR compliant. A high level of compliance requires that all procedures is implemented in the business and incorporated as part of the usual business processes.

In PwC's assessment, the increased efforts to protect personal data are mainly brought about by two factors: One is that customers and citizens have become increasingly aware of data protection and their rights, and the other is that the Danish Data Protection Agency has published a number of recommendations for reports to be made to the police. Personal data breaches in particular, which are required to be reported to the Danish Data Protection Agency, often lead to greater scrutiny of organisations' security of processing, which may result in a serious case at the Agency.

PAVA

Process

Organisations continue their work on documenting security and statutory requirements

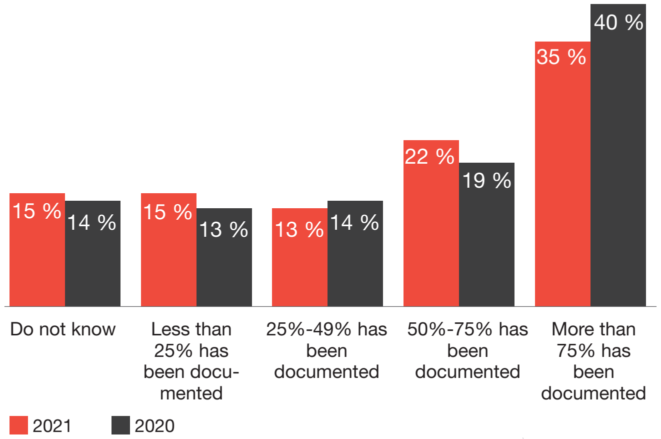
As in last year's Cybercrime Survey, this year's survey shows that organisations continue their work on documenting security and statutory requirements.

This work will contribute to, in part, the integration and compliance of internal procedures and guidelines within the organisations and in part the documentation of organisations' compliance with the requirements of authorities and customers.

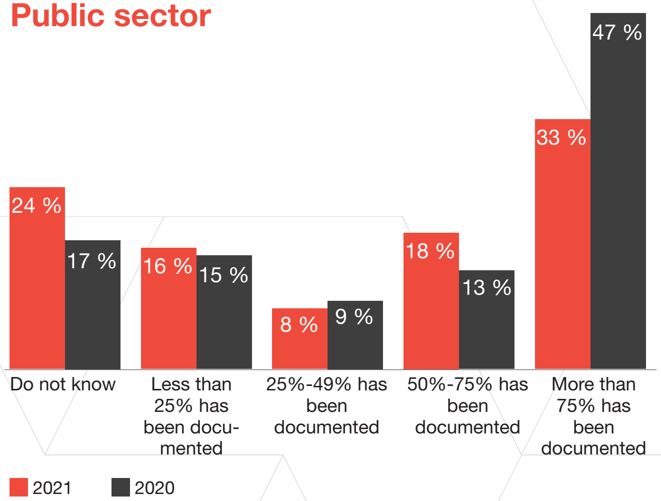
Just over half (57 %) of the respondents this year report that more than 50 % of their processes have been documented, which is roughly on par with 2020 (59 %). Compared to last year, there has been a slight decrease in the number stating that ”more than 75% has been documented”.

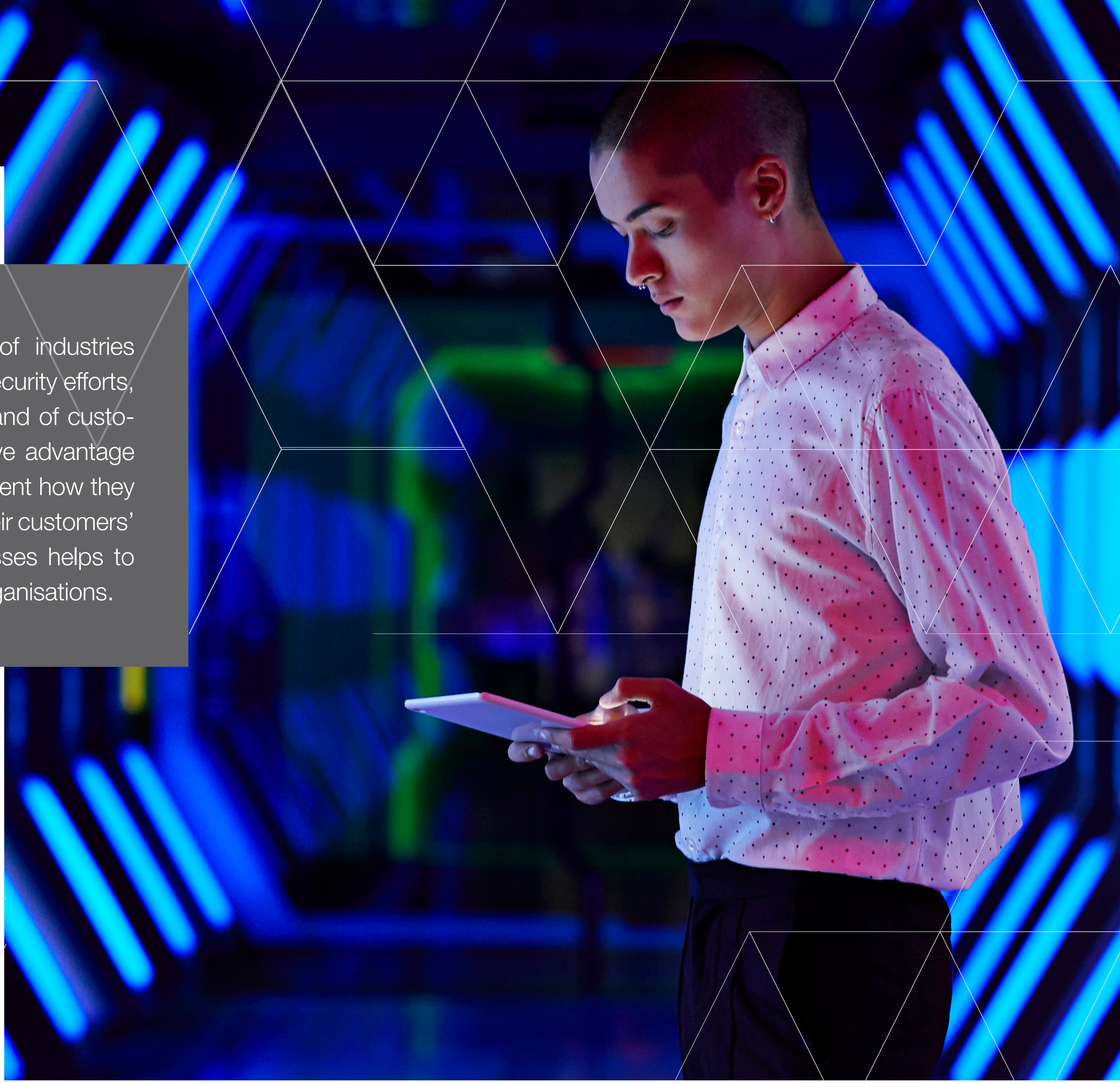
The decrease is partly due to the fact that, in 2021, fewer people in the public sector estimate that more than 75 % of their processes have been documented. Thus, almost half (47 %) of the public sector respondents in 2020 answered that more than 75% had been documented. In 2021, it is just one in three.

To what extent are security and statutory requirements documented in your organisation's internal policies, procedures and/or guidelines?



Public sector





PwC is seeing an increasing number of industries requiring documentation of organisations' security efforts, both as a result of statutory requirements and of customer inquiries. Thus, it may be a competitive advantage for some organisations to be able to document how they work with security and in that way protect their customers' data. In addition, documentation of processes helps to ensure integration and standardisation in organisations.

PAVA

Behaviour

PwC's e-learning courses

PwC has developed a number of e-learning modules on the EU General Data Protection Regulation ('GDPR') and cybersecurity which help train employees in an efficient and simple way.

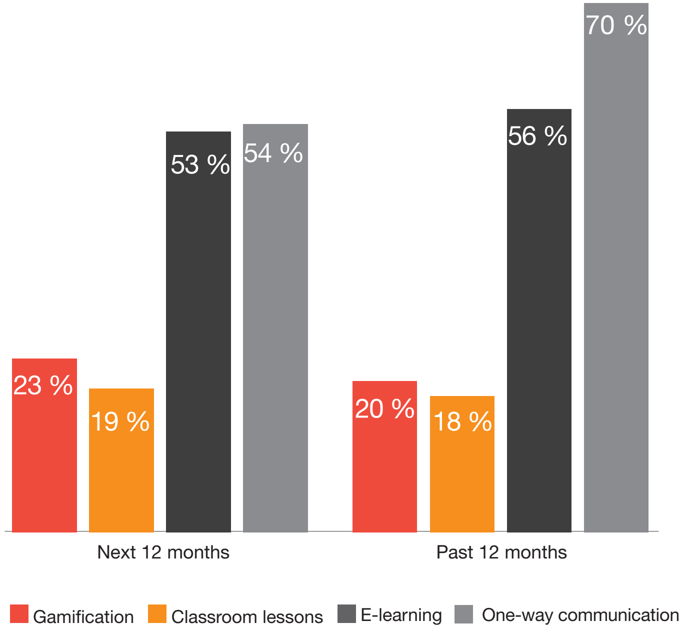
Read more at www.pwc.dk/cyberaware

Organisations focus on training of employees

Awareness training is to contribute to making employees aware of digital threats and risks that may have consequences for the organisation, customers or citizens.

In this year's survey, 7 out of 10 of the respondents replied that, in the past 12 months, they have used one-way communication to create awareness about cyber and information security. In the next 12 months, however, only 54 % expect to use one-way communication. One initiative that is of increasing interest to organisations is gamification. 23 % of respondents state that, in the coming 12 months, they will make use of this initiative whereas, in 2020, the number was 15 %. Over the past 12 months, 20 % has made use of gamification, which is 5 percentage points higher than expected in 2020.

Which of the following initiatives has your organisation introduced in connection with GDPR awareness and cyber and information security?



PwC recommends, that organisations continue to prioritise training and education of their employees in cyber and information security so that employees are able to prevent and detect cybercrime incidents. Training may for instance take place through e-learnings, activating the employees and providing them with an increased understanding of cybersecurity.

PAVA

Validation

Record-breaking level of threat from organised criminals

n 2021, organised criminals continue to pose the greatest threat to Danish businesses.

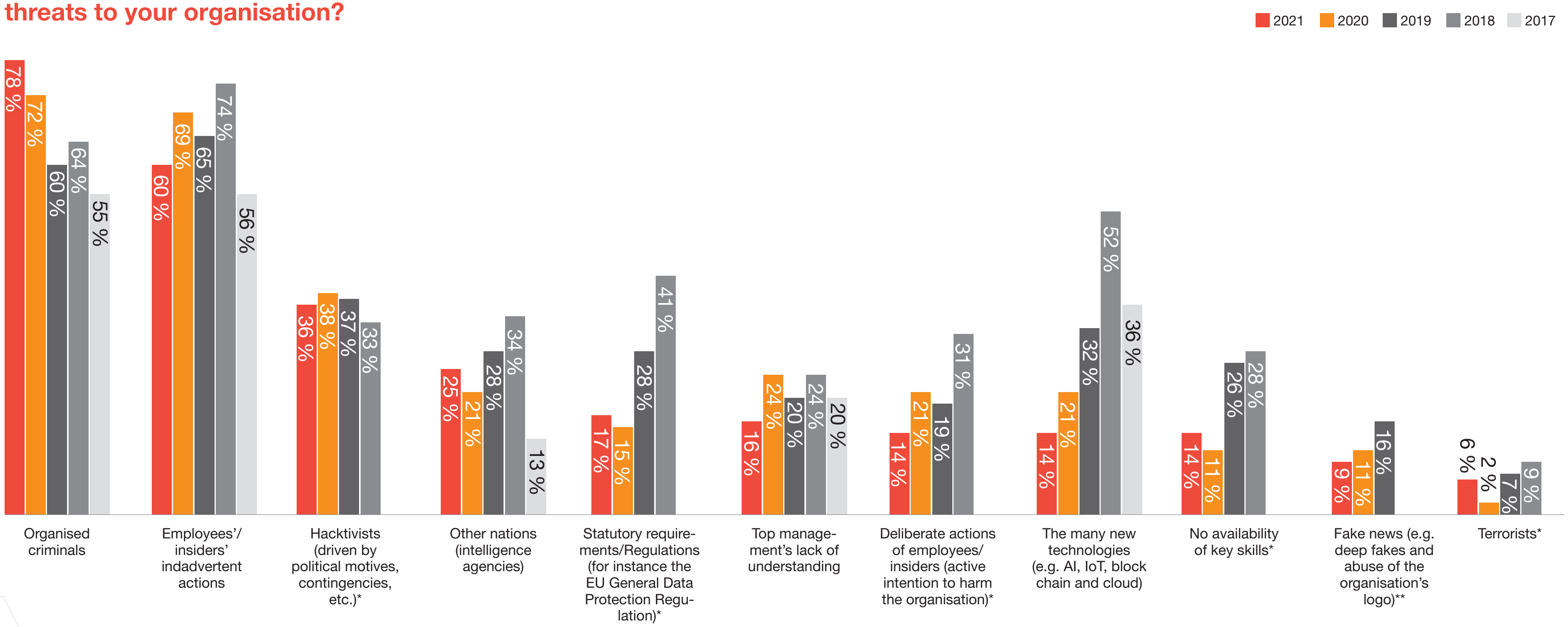
As many as 78% of respondents consider organised criminals to be among the greatest cyber threats, which is the PwC Cybercrime Survey's highest percentage so far. By comparison, the figure was 72% in 2020, and we have seen a steady increase in the percentage in recent years (from 55% in 2017).

However, the number of respondents stating the threat posed by the inadvertent actions of employees/insiders has decreased by 9 percentage points from 2020 to 2021, which is positive, given that organisations now have awareness training as their top investment priority for the third year in a row.

However, the threat from the inadvertent actions of employees/insiders is still real, which is underlined by the survey once again demonstrating that organisations are, to a great extent, exposed to phishing attacks. This year, 78% of respondents report that their organisation has experienced a phishing attack in the past 12 months.

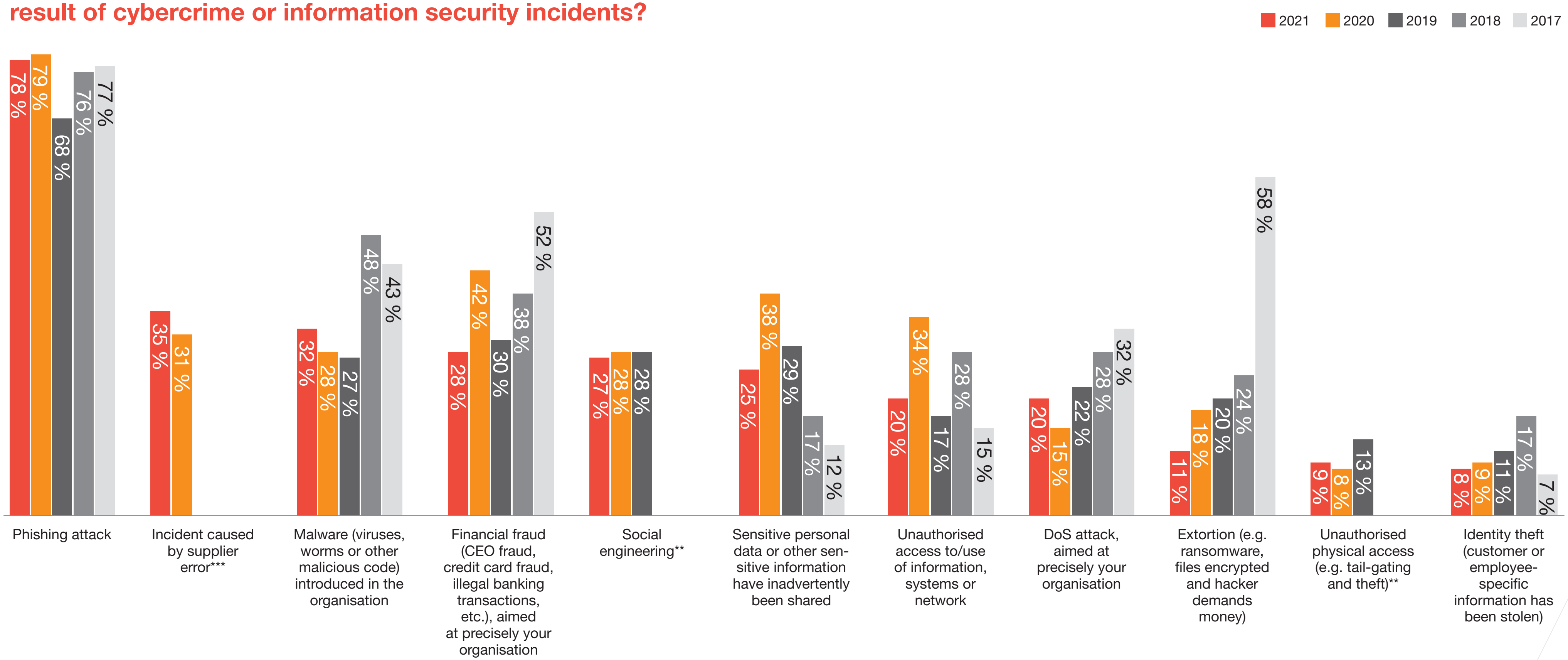
It is worth emphasising that fewer (38% in 2020 on 25% in 2021) state to have experienced an incident involving the accidental sharing of sensitive personal data or other sensitive information. This may also be linked to the organisations' continuous intention to prioritise awareness training.

What are the greatest cyber and information security threats to your organisation?



*This response option was added in 2018.
**This response option was added in 2019.

What incidents has your organisation experienced in the past 12 months as a result of cybercrime or information security incidents?



**This response option was added in 2019.
***This response option was added in 2020.

PwC experiences that cyber attacks, cyber attacks are characterised by cyber criminals acting more and more professionally. Hacker groups specialise and develop their methods of attack. Some cyber criminals specialise in phishing attacks for the purpose of gaining access to an identity. Others specialise in carrying out ransomware attacks, and if gaining sufficient access rights through the phishing attack, they will be able to access critical data and systems.

PAVA

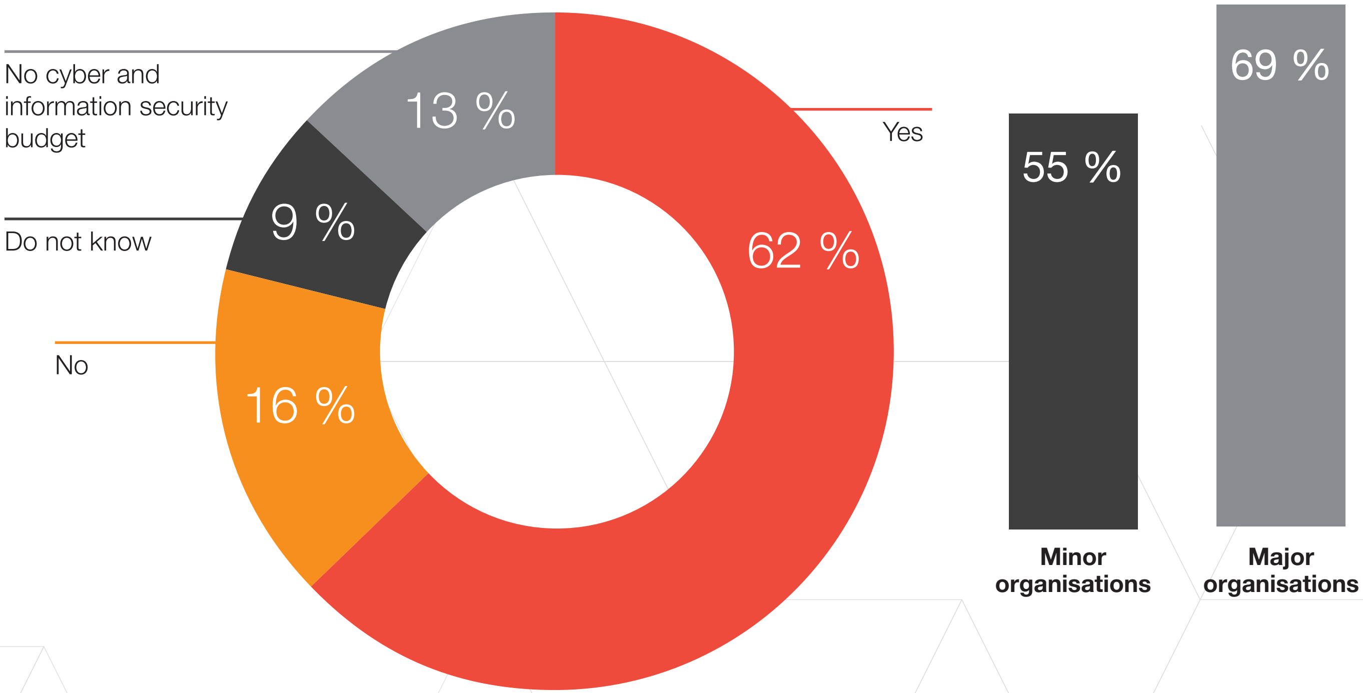
Architecture

2 out of 3 expect their cybersecurity budget to grow within the next 12 months

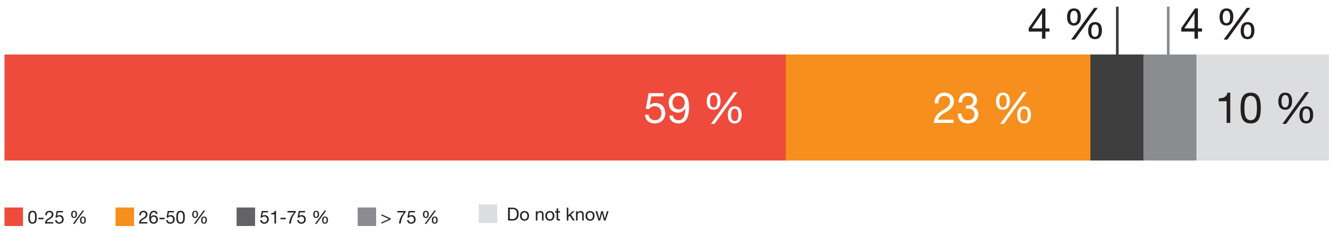
This year's Cybercrime Survey asks about organisations' expectations for their future cyber and information security budgets.

As many as 62% of respondents state that their organisations expect their cyber and information security budgets to grow within the next 12 months. 69% of the major organisations expect their budget to increase, while 55% of the minor organisations also expect an increase in their cybersecurity budgets.

Do you expect/think that the organisation's cyber and information security budget will grow within the next 12 months?



How much do you expect the cyber and information security budget to grow in the next 12 months?



Of these, 6 out of 10 expect the budget to increase by up to 25%, while 3 out of 10 expect a budget increase of more than 25%.

When asking about respondents' priority investments in cyber and information security over the next 12 months, the survey shows that this year's record breaker is awareness training (55 %), just like in previous years.

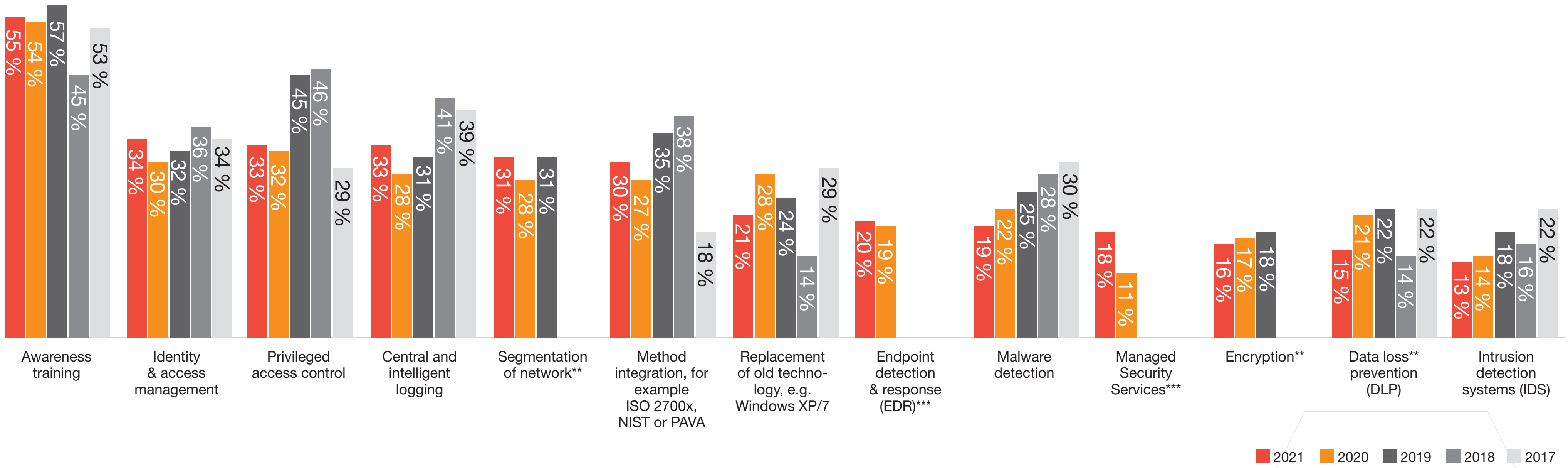
Second to awareness training comes identity and access management[4] (34 %), privileged access management[5] (33 %) and central and intelligent logging[6] (33 %) take second and a shared third place, respectively, which is very similar to the picture in 2020. PwC points out that these top 3 investments have all increased since 2020.

[4] Identity and access management (IAM) is about structuring and automating all identities in an organisation, including ensuring correct allocation and cancellation of rights in a timely manner.

[5] Privileged access management (PAM) is about handling the privileged rights to an organisation's infrastructure.

[6] Central and intelligent logging is about logs being collected for a central platform, which is subsequently analysed by an automated system (e.g. SIEM).

What are your organisation's highest-priority investments within IT security over the next 12 months?



**This response option was added in 2019.
***This response option was added in 2020.

PwC has in recent years learnt that Danish management teams and boards are more aware than they were in the past of the risks arising from cybercrime. This applies not only to large but also to medium-sized organisations in all industries. The interest has brought about increased investments in dedicated initiatives intended to help reduce the risks of cybercrime. Moreover, actual cyber programmes are established with carefully aligned and approved budget figures.

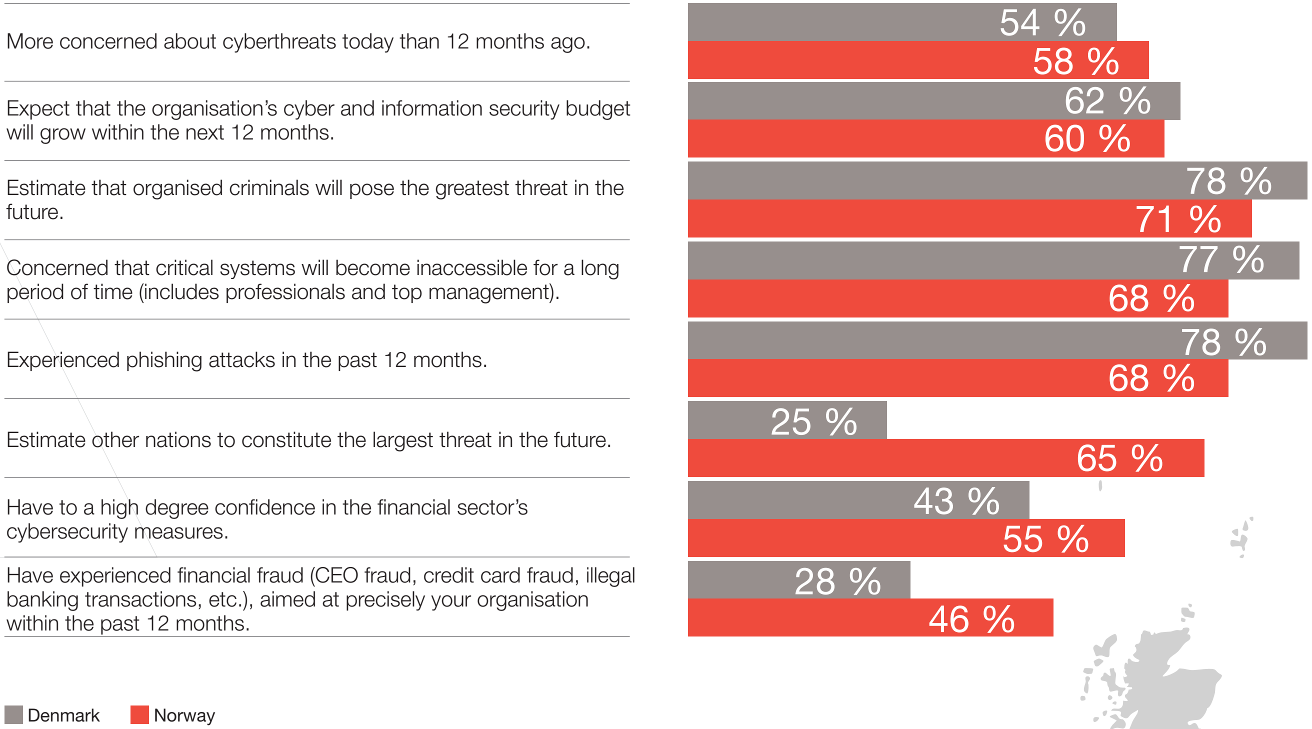
A Norwegian perspective

Through PwC's Cybercrime Survey 2021, Norwegian IT managers and security specialists shared their views on a number of questions related to cybersecurity.

Overall, concerns about cyber threats are on the rise, with more than half of respondents (Denmark: 54 %, Norway: 58%) reporting to be more concerned about cyber threats today than they were a year ago – similarly, the majority of respondents in both countries expect an increase in their cybersecurity budgets within the next year (Denmark: 62 %, Norway: 60 %). As is the case with the threat landscape in Denmark, organised criminals are considered the greatest threat in Norway (Denmark: 78 %, Norway: 71 %). The main concern in respect of the consequences of a cyber incident is – as in Denmark – that critical systems become unavailable for a long period of time (Denmark: 77 %, Norway: 68%).

The Danish and Norwegian responses differ in terms of the assessed threat from other nations, as the Norwegian respondents list this threat more than 2.5 times more often than Danish respondents (Denmark: 25 %, Norway: 65 %).

Moreover, the number of organisations exposed to financial fraud differs. Almost half (46 %) of the Norwegian respondents have been subject to CEO fraud, credit card fraud, illegal banking transactions, etc. In comparison, 28 % of the Danish respondents state the same.



About the survey

A great thanks to this year's partners and executives, IT managers and security specialists who have contributed to this year's PwC Cybercrime Survey, thereby helping to highlight cybersecurity in Danish businesses and public institutions.

As many as 402 Danish and 119 Norwegian business executives, IT managers and security specialists participated in PwC's Cybercrime Survey 2021. The survey has yet again been completed with the support of the Centre for Cyber Security, DI Digital, Finance Denmark, the Danish Chamber of Commerce, ICT Industry Association, the Danish IT Society, KITA, the Digital Security Council, ISACA, Microsoft, DK Hostmaster and the Board Leadership Society. The analysis is based on online responses.

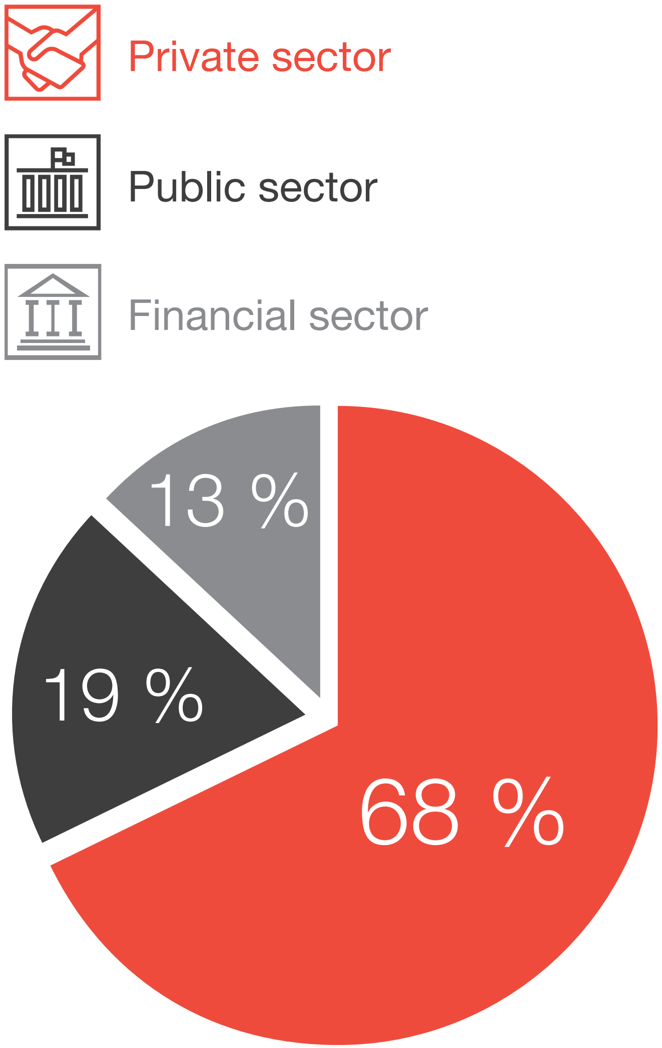
Respondents were asked a number of questions related to the cyber area, such as whether they have been hit by a cyber attack, whether they expect their cyber and information security budget to increase, and what investments have been given top priority.

The questions and answers of the analysis were prepared by PwC and the online questionnaire was issued in collaboration with the above organisations.

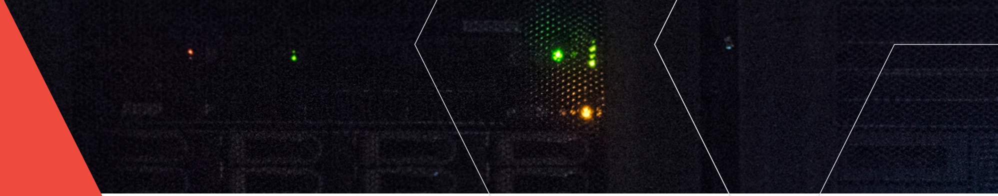
Major organisations are defined as ≥ **200** employees.

Minor organisations are defined as ≤ 199 employees

Survey respondents divided by sector:



Checklist



PwC wants to help organisations take the best precautions against the cyber threat, both before, during and after an attack. As there are many and often complex solutions, PwC has prepared the list below to help organisations decide on some of the key target areas for cyber and information security.

Governance, risk and compliance

- □ Have you established a formal security committee with representatives from the organisation's top management?
- □ Are other cyber and information security roles defined, allocated and communicated?
- □ Do you work in a structural manner with risk assessment based on security threats, vulnerabilities and consequences for the business?
- □ Is the organisation's security status reported continuously to the organisation's management board/board of directors?
- □ Do security assignments include both information security (ISO 27001) and cybersecurity? Read more at pwc.dk/iso27001
- □ Have you implemented the GDPR?
- □ Has an operational organisation been established to continue ensuring compliance with the GDPR?

Processes

- □ Have you measured your resilience against cyber threats (cyber assessment)?
- □ Have you documented and communicated the processes for all security areas?

Behaviour

- □ Has a programme been set up in regard to continuous training of and communication to employees about security?
Read more at www.pwc.dk/cyberaware

Validation

- □ Are you conducting continuous tests to identify vulnerabilities in your infrastructure and systems?
- □ Do you have a defined and tested incident response process? Read more at www.pwc.dk/response
- □ Have you tested your business continuity plan for cyber incidents? Read more at pwc.dk/beredskab

Architecture

- □ Do you have a plan for implementation of security technology?
- □ Do you have a process and plan for compliance with privacy by design, including implementation of a security architecture? Read more at pwc.dk/iam og pwc.dk/pam

Get more tips and tricks on cyber incident response

Are you a CFO or part of Management? The CFO's Cyberguide takes you through the steps of building a strategic cyber incident response for your business.

Read more at www.pwc.dk/cfocyberguide

Contact

About PwC

Our purpose is to build trust in society and solve important problems. We do so based on our knowledge of audit, tax and advisory services. Our clients come from all parts of the business community and the public sector, and we are more than 2,500 partners and staff who are committed to making a positive difference for clients and colleagues. We have more than 276,000 colleagues in 157 countries and are a market leader in Denmark. Meet us throughout the country. We are where you are.

We would like to discuss the results of this year's Cybercrime Survey with you. Please contact one of PwC's experts for an informal talk about your specific challenges and needs. You can also read more about our cyber and information security services at www.pwc.dk/cyber

Mads Nørgaard Madsen
Partner
Head of Technology & Security

Technology & Security
T: 2811 1592
E: mads.norgaard.madsen
@pwc.com

Peter Brock Madsen
Partner
Cyber Risk Management

Technology & Security
T: 2056 8505
E: peter.brock.madsen
@pwc.com

William Sharp
Partner
Cyber Operational Technology

Technology & Security
T: 4040 1074
E: william.sharp@pwc.com

Christian Kjær
Partner
Cyber Incident Response

Technology & Security
T: 5132 1270
E: christian.kjaer@pwc.com

This publication does not constitute and should not replace professional advice. PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab assumes noliability for any loss suffered as a result of actions or failure to actbased on the contents of this publication, or for any content-related errors or omissions.

In this document, "PwC" refers to PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

Cyber Incident Response-Team

PwC helps clients prevent and manage cybersecurity incidents.

We have established a central cyber hotline for customers, allowing you to get instant assistance. PwC's team of experts will help you create an overview of focus areas in relation to the specific threat, and our cyber forensics specialists identify the nature of the attack and the vulnerabilities exploited. Subsequently, we will implement security improvements and prepare a report for management, the insurance company, the Danish Data Protection Agency and the police.

Read more at
www.pwc.dk/response

pwc

PwC's cyber hotline

+45 70 222 444

pwc

FSC
www.fsc.org
MIX
Papir fra
ansvarlige kilder
FSC® C009089

ClimateCalc
Denne tryksag er klimakompenseret i henhold til ClimateCalc.
Kompensation er købt hos: Gold Standard
www.climatecalc.eu
Cert. no. CC-000004/DK

NORDIC SWAN ECOLABEL
Printed matter
5041-0492

Audit. Tax. Advisory.

Together we succeed ...