Dear participant,

We are pleased that you are taking part in our study related to the status of cybersecurity in Denmark. Your opinion is very important to us, and by participating you will make a valuable contribution to our research.

This survey will take approximately 10 minutes to complete.

The survey is conducted as a part of the ASCD research project (see https://ascd.dk for more details), which is a collaboration between the IT University of Copenhagen (ITU) and Southern Denmark University (SDU). The aim of the survey is to investigate the status of cybersecurity among Danish companies in order to identify the challenges companies face and look into possible solutions for these challenges. For this purpose you will be asked questions about the security and privacy practices in your company. **We will use your responses for research purposes only.** Our research team will only have access to the responses you provided yourself within the survey. We will only share the data from the survey, including publishing the results of the survey analysis in project reports and academic publications, in anonymised or aggregated form.

For more information about the survey, feel free to contact us using either the email addresses below or the contact form at https://ascd.dk/contact/. More information about data protection by ITU and SDU of the data from the survey responses is available at https://ascd.dk/data-protection/. If you have more questions or requests about the processing of your personal data, please contact our data protection officer at dpo@itu.dk.

Responsible for the study are:

Dr. Oksana Kulyk, ITU (okku@itu.dk)

Dr. Jacopo Mauro, SDU (mauro@imada.sdu.dk)

By pressing the ”Next” button, you freely and knowingly accept that you have read and understand the provided information and have had the opportunity to ask questions. You understand that your participation is voluntary and that you are free to withdraw at any time, without giving a reason and without a cost.

What are your responsibilities in your organization?

Select one or more

(1) ❑ Management related tasks
(5) ❑ IT-security related tasks
(6) ❑ Privacy/data protection related tasks
(2) ❑ Software development related tasks
(4) ❑ IT administrator related tasks
(3) ❑ Other, please specify _____

Organisation profile

We'll start with some questions about your organisation.

How many employees are there in your organisation?

(1) ❑ Less than 10

(5) ❑ 10 - 50

(6) ❑ 51 - 250

(4) ❑ More than 250

What industry sector is your organisation in?

(1) ❑ Media & Publishing

(4) ❑ Health care

(5) ❑ Financial services

(6) ❑ Software development

(7) ❑ Entertainment & Music

(8) ❑ Education

(9) ❑ Manufacturing

(10) ❑ Consultancy

(12) ❑ Life Sciences and Pharmaceuticals

(13) ❑ Insurance

(11) ❑ Other

In which countries does your organisation have branches?

Select one or more

(1) ❑ Denmark

(5) ❑ Other Nordic countries

(7) ❑ Other EU countries (non-Nordic)

(8) ❑ Non-EU countries

What is your organisation's turnover (in DKK)?

(1) ❑ Less than 500k
(3) ❑ 500K - 500M
(4) ❑ 500M - 1B
(5) ❑ More than 1B
(6) ❑ Not sure

Security and privacy management

The following questions will ask about your general practices in managing security and privacy in your organisation, including security and privacy standards and policies, data protection and response to cyber attacks.

Do you have a yearly budget allocated for Security & Privacy needs?

(1) ❑ Yes
(2) ❑ No
(3) ❑ Not sure

If YES, what percentage of your IT budget does it constitute?

(1) ❑ Less than 1%
(2) ❑ 1% - 3%
(3) ❑ 3% - 5%
(4) ❑ More than 5%
(5) ❑ We don't have a defined security budget
(6) ❑ Not sure

To what extent your organization has outsourced IT systems and IT security?

(1) ❑ We have outsourced all of our IT systems, including IT-security
(2) ❑ We have outsourced parts of our IT systems, but handle IT-security internally
(3) ❑ We have outsourced parts of our IT systems, and also parts of IT-security
(4) ❑ We have not outsourced any IT systems and IT-security, it is all handled internally

How do you measure your cyber-security and privacy readiness?

Select one or more

(1) ❑ We rely on the IT solutions derived from established security and privacy standards
(2) ❑ Internal method/ framework/ procedure
(3) ❑ We do not have any measures
(4) ❑ Not sure

If you rely on established standards to measure your cyber-security and privacy readiness, which ones do you use?

Select one or more

(1) ❑ ISO/IEC 27001
(16) ❑ ISO 27701
(2) ❑ Center for Internet Security - Critical Security Controls (CIS CSC)
(3) ❑ Control Objectives for Information and Related Technologies (COBIT)
(4) ❑ Security for Industrial Automation and Control Systems (ANSI/ISA-62443)
(5) ❑ NIST Special Publication 800-53 (NIST SP 800-53)
(6) ❑ Payment Card Industry Data Security Standard (PCI DSS)
(7) ❑ UK National Cyber Security Centre (NCSC) 10 Steps
(8) ❑ UK National Health System (NHS) Digital Data Security and Protection Toolkit
(9) ❑ Cyber Assessment Framework (CAF)
(10) ❑ Information Assurance Small and Medium Enterprises (IASME)
(11) ❑ Host-Based Security System (HBSS)
(12) ❑ Structured Threat Information Expressions (STIX)

(13) ❑ Assured Compliance Accreditation Solutions (ACAS)

(14) ❑ Cyber Federated Model (CFM)

(15) ❑ Other, please specify _____

How is your security and privacy practice defined?

Select one or more

(1) ❑ Practices to be followed defined at the company level

(3) ❑ Practices to be followed defined at the project level

(5) ❑ Practices improved based on previous experience/ projects

(6) ❑ Other, please specify _____

Are the methods/ practices/ standards of the company, always followed in all the situations?

(1) ❑ Yes

(2) ❑ No

(3) ❑ Not sure

If NO, why?

Select one or more

(1) ❑ They are not always compatible with the functional requirements of our products

(2) ❑ I feel that they are not very helpful in protecting security and privacy

(7) ❑ They interfere with other workflows in the organisation

(3) ❑ They are too complicated to follow exactly as defined

(4) ❑ We don't have time or resources to follow them exactly as defined

(5) ❑ The management does not think they should be followed exactly as defined

(6) ❑ Other, please specify _____

What kind of information do you gather when investigating a cyber-security incident?

Select one or more

(1) ❑ Network (MAC/IP addresses, domains, and/or packet data)
(2) ❑ Operating system (type and version)
(3) ❑ Execution logs
(4) ❑ Login/logout logs
(5) ❑ Temporary files
(6) ❑ Device (identifiers and related information)
(7) ❑ Closed-circuit recordings
(8) ❑ Key-logs
(9) ❑ E-mails
(10) ❑ Browser history
(11) ❑ Sensor data
(12) ❑ Memory data
(13) ❑ Other, please specify _____

Which policies are adopted to prevent security and privacy problems working remotely?

Select one or more

(1) ❑ Doing work only through the organisation's VPN
(2) ❑ Having personnel working only on organisation-provided devices
(3) ❑ Ensuring that the data from these services is only stored within the organisation IT infrastructure
(4) ❑ Making sure there is a data agreement with the providers of the remote work services
(5) ❑ Other, please specify _____

Has anything in the security and privacy practices of your organisation changed since the introduction of the GDPR regarding the following aspects?

	Yes	No	Not sure
Which data is collected by the organisation	(1) ❑	(2) ❑	(3) ❑

	Yes	No	Not sure
How the data subjects are informed about data collection	(1) ❑	(2) ❑	(3) ❑
How the collected data is stored	(1) ❑	(2) ❑	(3) ❑
How the collected data is shared	(1) ❑	(2) ❑	(3) ❑
How the collected data is deleted	(1) ❑	(2) ❑	(3) ❑
Which controls are provided to the data subjects	(1) ❑	(2) ❑	(3) ❑

Does your organisation collect personal data of people outside the organisation (e.g. users, customers, suppliers etc.)

(1) ❑ Yes, only personal non-sensitive data
(2) ❑ Yes, only personal sensitive data
(3) ❑ Yes, personal sensitive and non-sensitive data
(4) ❑ No
(5) ❑ Not sure

If your organisation collects personal data, what controls over the collected data are provided to the data subjects?

Select one or more

(1) ❑ Request an overview of data collected from them
(2) ❑ Request to delete the data collected from them
(3) ❑ Request to correct the data collected from them
(4) ❑ Decide which data they want to share
(5) ❑ Other, please specify _____

Development practices

The next set of questions concerns the development practices in your organisation.

Which development method you use (in part or whole) at your company?

Select one or more

(1) ❑ Classic Waterfall
(3) ❑ Iterative development
(4) ❑ V-shaped model
(5) ❑ Spiral
(6) ❑ Scaled Agile (SAFe)
(7) ❑ Large-Scale Scrum
(8) ❑ Lean Development
(9) ❑ XP
(10) ❑ Kanban
(11) ❑ Devops
(12) ❑ Other, please specify _____

What is your frequency of software releases? (e.g., Major releases, Minor releases)

Select one or more

(1) ❑ Less than one day
(2) ❑ Between one day and one week
(3) ❑ Between one week and one month
(4) ❑ More than a month
(5) ❑ Not sure

When do you integrate security/ privacy into your development practices?

(1) ❑ Early, from the initial phases
(2) ❑ Continuously during the development cycle
(3) ❑ After the fact
(4) ❑ Not at all
(5) ❑ Other, please specify _____

Do you use any of these tools/ procedures to ensure software reliability, security, and privacy?

	Yes	No	Don't know
Simulation	(12) ❑	(13) ❑	(14) ❑
Testing	(12) ❑	(13) ❑	(14) ❑
Performance analysis and profiling	(12) ❑	(13) ❑	(14) ❑
Core review	(12) ❑	(13) ❑	(14) ❑
Formal verification	(12) ❑	(13) ❑	(14) ❑
Intrusion detection systems	(12) ❑	(13) ❑	(14) ❑
Circuit breakers, load balancers, network isolation	(12) ❑	(13) ❑	(14) ❑
Permission management	(12) ❑	(13) ❑	(14) ❑
Safe-by-design programming languages (e.g., Rust, Haskell)	(12) ❑	(13) ❑	(14) ❑
Blameless post-mortem meetings	(12) ❑	(13) ❑	(14) ❑
Peer-review	(12) ❑	(13) ❑	(14) ❑
Penetration testing	(12) ❑	(13) ❑	(14) ❑
Blu-Red Team exercises	(12) ❑	(13) ❑	(14) ❑
Dev(Sec)Ops	(12) ❑	(13) ❑	(14) ❑
Site Reliability Engineering	(12) ❑	(13) ❑	(14) ❑

	Yes	No	Don't know
Anonymisation of data	(12) ❑	(13) ❑	(14) ❑
Pseudonymisaton of data	(12) ❑	(13) ❑	(14) ❑
Encryption	(12) ❑	(13) ❑	(14) ❑
Timely deletion of data	(12) ❑	(13) ❑	(14) ❑

Do you use any further tools/ procedures to ensure software reliability, security, and privacy?

(1) ❑ Yes, namely : _____

(2) ❑ No

Are the methods/practices /standards for security and privacy protection in the development processes, always followed in all the situations?

(1) ❑ Yes

(2) ❑ No

(3) ❑ Not sure

If NO, why?

(1) ❑ They are not always compatible with the functional requirements of our products

(2) ❑ I don't believe that they are helpful in protecting security and privacy

(7) ❑ They interfere with other workflows of my tasks and responsibilities

(3) ❑ They are too complicated to follow exactly as defined

(4) ❑ We don't have time or resources to follow them exactly as defined

(5) ❑ The management does not think they should be followed exactly as defined

(6) ❑ Other, please specify

General security and privacy practices

The following questions are concerned with the general security and privacy policies applied in your organisation.

Which of these behaviours have you practiced yourself or observed among your colleagues?

Select one or more

(1) ❑ Sharing passwords with friends/ colleagues
(2) ❑ Using passwords that are not secure (e.g., less than 12 characters or using family names or dates of birth)
(3) ❑ Using the same password for multiple systems
(4) ❑ Using personal online storage systems to exchange and/or keep work-related data
(5) ❑ Using free-to-access public Wi-Fi to work or with a device containing work-related data
(6) ❑ Downloading programs from the Internet without the authorisation of the IT department
(7) ❑ Disabling the anti-virus on work computers to download or run programs from the Internet
(8) ❑ Accepting friend requests on social media from unknown people
(9) ❑ Clicking on links contained in unsolicited emails or from an unknown source
(10) ❑ Sending information (personal, work-related) to strangers over the Internet

What kind of assets of your organisation can be susceptible to a cyber-attack?

Select one or more

(1) ❑ Customers' and/or suppliers' data
(2) ❑ Intellectual property
(3) ❑ IT infrastructure
(4) ❑ Social media accounts
(5) ❑ Physical systems (health, transportation, goods)
(6) ❑ Our website
(7) ❑ Employees' data
(8) ❑ Other, please specify _____

How familiar are you with the security and privacy policies your organization wants you to follow?

(1) ❑ I am familiar with all of them
(2) ❑ I am familiar with most of them
(12) ❑ I am not familiar with most of them
(3) ❑ I am not familiar with any of them

If you are familiar with the security and privacy policies, how challenging are they to follow?

(1) ❑ Very challenging
(2) ❑ Mostly challenging
(4) ❑ Mostly not challenging
(5) ❑ Not at all challenging

If you are familiar with the security and privacy policies, how helpful do you think are they in protecting against security and privacy risks?

(1) ❑ Not at all helpful
(2) ❑ Mostly not helpful
(4) ❑ Mostly helpful
(5) ❑ Very helpful

What is your experience with security and privacy awareness trainings at your company?

(1) ❑ I participated in trainings and found them useful
(2) ❑ I participated in trainings and did not find them useful
(3) ❑ I heard about available trainings but did not participate in them
(4) ❑ I am not aware of any security and privacy trainings at my organisation
(5) ❑ Prefer not to answer

To what extent has pandemic affected your working style, in particular remote working?

(1) ❑ I worked remotely before the pandemic and work remotely to the same extent now

(2) ❑ I started working remotely during the pandemic, but now I'm working completely in office

(3) ❑ I started working remotely during the pandemic and I'm still continuing to work remotely

(4) ❑ I haven't worked remotely during the pandemic

If you started working remotely after the pandemic, how challenging do you find it to comply to the security and privacy policies of your organisation regarding remote work?

(1) ❑ Not at all challenging

(2) ❑ Mostly not challenging

(4) ❑ Mostly challenging

(5) ❑ Very challenging

(7) ❑ There are no security and privacy policies regarding remote work in my organisation

(6) ❑ I am not aware what the security and privacy policies regarding remote work are in my organisation

How did your concerns regarding security and privacy in your organizations change because of the pandemic?

(1) ❑ I am more concerned now than I was before the pandemic

(2) ❑ I am concerned, but my concerns have not changed because of the pandemic

(3) ❑ I am less concerned now than I was before the pandemic

(4) ❑ I am not at all concerned, regardless of the pandemic

Do you know how to report a security and privacy incident (such as a cyber attack or a data leak) in your organisation?

(1) ❑ Yes

(4) ❑ No

(3) ❑ Not sure

(5) ❑ Prefer not to answer

What kind of information do you gather when investigating a cyber-security incident?

Select one or more

(1) ❑ Network (MAC/IP addresses, domains, and/or packet data)
(2) ❑ Operating system (type and version)
(3) ❑ Execution logs
(4) ❑ Login/logout logs
(5) ❑ Temporary files
(6) ❑ Device (identifiers and related information)
(7) ❑ Closed-circuit recordings
(8) ❑ Key-logs
(9) ❑ E-mails
(10) ❑ Browser history
(11) ❑ Sensor data
(12) ❑ Memory data
(13) ❑ Other, please specify _____

Your organisation's name:

_____

If you want, you can provide us with the name of your organisation. **This information is strictly optional.** The purpose of having this data is to have a possibility to have a follow-up study to get a deeper understanding on cybersecurity challenges. **We will not share the name of your organisation with anyone and will only store it for the duration of the project.** If you change your mind about providing us with the name of your organisation, please contact us at https://ascd.dk/contact/.

Thank you for your participation!
Please click on the "Finish" button to complete the survey. If you have questions about the project, feel free to contact us via the contact form on the project website (https://ascd.dk/contact/).