Charter of Trust

Seeing cybersecurity as an opportunity

How to protect your business effectively: specific measures for small and medium-sized enterprises

Why are you particularly vulnerable?

In this era of global integration, cybercrime is an ever-growing challenge that no one can overlook. The facts and figures on this page illustrate this vividly. Small and medium-sized enterprises are particularly vulnerable. But it doesn't have to be that way: By introducing just a few specific measures, you can take some decisive steps that will not only enhance your company's security, but also seize new business opportunities. This brochure shows you how. Keep reading – and read the latest updates at:

www.charteroftrust.com/topics/education

43.4 billio

Total losses sustained by German businesses from cybercrime in the past two years. [1]

68%

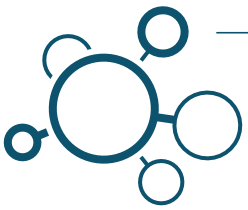
of companies with 10 to 99 employees have been victims of espionage, sabotage, or data theft in the past two years.[2]

46%

of these companies were harmed by cyberattacks during the same period.[3]

390,000

new types of malware, such as ransomware, are discovered daily.[4]

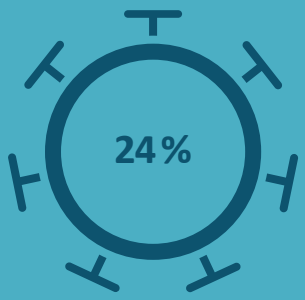


n euros

What is the role of humans?

Cyberattacks launched on small and medium-sized companies in particular are generally discovered by employees. The human factor is therefore an elementary part of the process. By focusing company-wide on cybersecurity, raising employee awareness levels about the issue, and providing training, you can take an action that will bolster your company's line of cyberdefense. After all, conscious and critical behavior in the digital world creates security and trust – and that pays off. On the other hand, human beings also remain the primary gateway for cybercriminals. Carelessness can endanger your company, as the numbers on this page clearly show. Assume your responsibility and create this level of awareness. In doing so, you will take the first important step toward improving cybersecurity at your company.

Source of losses from cyberattacks in the past two years[5]



Malware (malicious software)

Software vulnerabilities	**16 %**
Phishing attacks	**16 %**
Attacks on passwords	**12 %**
Spoofing	**6 %**
DDOS attacks	**5 %**
Man-in-the-middle attacks	**4 %**

38 %

IT (Administration / Service)

Business areas (presumably) affected by data theft, industrial espionage, or sabotage in the past two years [7]

28 %

Management

24 %

Production / manufacturing

14 %

Research and development

How did companies with 10 to 99 employees affected by data theft, industrial espionage, or sabotage in the past two years learn about the incidents? [6]

In-house security system / virus scanner / firewall

38 %

65 %

Tips from people inside the company (individuals)

How can small or medium-sized companies like yours take advantage of cybersecurity?

Turn cybersecurity into a success factor.

As digital integration grows more widespread, cybersecurity is becoming a genuine guarantor of success. That's because cybersecurity is not merely the response to a threat: If consistently promoted, it offers a real opportunity to enhance your own **competitiveness.**

Cybersecurity, when implemented systematically, creates many positive effects – for every company. It ensures better **reliability** in your supply chains, it protects your ongoing operations, and it strengthens your **trustworthiness** with your customers by allowing you to handle their sensitive data responsibly. This security enhances the quality of the products and services you provide, making your portfolio more attractive and strengthening your competitive position on the markets.

Reliability

+

Trustworthiness

=

Competitiveness

You can improve your cybersecurity in three steps

Cybersecurity is a complex challenge that requires a targeted organizational, technical, and personnel-driven response. To use a sports analogy: It's not a sprint, it's a marathon. But even the longest journey begins with the first step.

That is why we have divided the brochure into three individual steps – which we call phases. Join us on this journey. You'll quickly see that each individual step brings you closer to your goal.

Other important sources of information:

www.bsi.bund.de/EN
www.allianz-fuer-cybersicherheit.de
https://english.bdi.eu/topics/global-issues/cyber-landscapes/
www.enisa.europa.eu
www.weforum.org/centre-for-cybersecurity

Phase 1 Identify threats and assume responsibility

A Practice responsibility

B Heighten awareness of security risks

C Cultivate a cybersecurity culture in your organization

Phase 2 Take action and embed security

A Embed cybersecurity within the organization

B Embed cybersecurity within products and services

Phase 3 Make the structure of cybersecurity transparent, and be a role model for others

A Publish your own cybersecurity setup

B Become active – even outside your own company

Phase 1 — A Practice responsibility

Define clear responsibilities for cybersecurity in your company.

Cybersecurity must be perceived and practiced at all levels – from the product and service level to the network level to the enterprise level, in the supply chain, and with the customer. That's why a comprehensive security strategy must address all levels of the company and the entire supply chain.

A strategic approach is needed, because the risks from cyberattacks can be so massive that, in the worst-case scenario, they can jeopardize the very survival of your own business or that of your customers.

Proper coordination of the various measures means establishing cross-divisional, cross-departmental responsibilities. **Make cybersecurity your top priority as the head of your company and create the position of cybersecurity coordinator (for instance, a chief information security officer)** who will handle all aspects of the work. You also need to make it clear to your employees, and particularly your managers, that they bear the primary responsibility for cybersecurity in your company. **Cybersecurity must be a defined aspect of work responsibilities and job descriptions for your entire management team.**

Regulate and manage responsibilities

Every business has multiple levels where cybersecurity counts.

A comprehensive security strategy encompasses not only every level of the company but also the entire supply chain.

1 Enterprise level — office network (IT)
Communication via internet and intranet, management of data in local and decentralized (cloud) systems

2 Productive level — production, IT/OT network
Data traffic and communication in the production systems in the IT/OT network and to some extent in networked devices (IoT, SCADA, ...)

3 Product level — products, systems, component
Hardware and software are created using products and systems, components and subsystems manufactured by suppliers and delivered to customers (cybersecurity requirements for the entire supply chain)

Supply chain

Customer enterprises

Supplier enterprises

Phase 1 — B
Heighten awareness of security risks

Make the risks from cyberattacks the center of your attention.

The risks to your business include the threats from cyberattacks, which is why they need to be incorporated into your company's risk management. The company's management can be responsible for this area, or it may be delegated to the coordinator for cybersecurity or the chief information security officer. Take the following steps:

Step 1:
Perform a proactive, enterprise-wide risk assessment – especially with regard to identifying critical business processes and critical data.

Step 2:
Evaluate the current threat landscape and the risk profile of your company. Then formally define your own willingness to take risks.

Step 3:
Develop an enterprise-wide plan for cybersecurity measures and cyberresilience and an internal communications strategy. Then, implement them across all departments and business units. Use the other recommendations in this brochure as your guide (for instance, regarding a cybersecurity culture) as well as the sources identified in it. Bring in external service providers as needed.

Step 4:
Monitor the effectiveness of the company's cybersecurity measures and cyberresilience and report to company management.

Regularly repeat the risk management cycle.

Phase 1 — C
Cultivate a cyber-security culture in your organization

Regularly train your employees and executives on cybersecurity issues.

A study by Accenture found that 60 percent of cyberattacks on companies result from the improper behavior of their own employees. This high figure alone shows how important it is to provide the workforce with cybersecurity training. Employees who have not learned how to avoid and handle security attacks cannot and must not hold any responsibilities for their company in the digital sphere.

If you skimp on providing the proper training, you run the risk of endangering your entire company in the event of an attack. It's also important to raise awareness among colleagues – akin to the value of good neighbors in the outside world: Vigilant neighbors protect you against burglaries, and vigilant colleagues protect you against attacks from cyberspace. That's why it's important to **regularly train your employees in best practices for cybersecurity.** Simple rules of conduct are enough to help your workforce stay safe in the digital sphere.

It's also critical that you continually hone your company's cybersecurity strategy. **Train selected employees to become cybersecurity experts.** Take advantage of the training courses offered by various organizations.

Fostering a cybersecurity culture – initial recommendations for all employees

Use different passwords and two-factor authentication for your accounts.

- Long, cryptic passwords with numbers, special characters, and both upper- and lowercase letters are more secure.
- Avoid simple strings of numbers or characters, real names, and complete words.
- Do not make your passwords accessible to others – by writing them down, for example.
- Use two-factor authentication with additional identification, such as a text message code.

Recognize fraudulent emails and be careful with attachments and links.

- Be suspicious of emails with unsolicited information or attachments and messages with a known name but unknown email address.
- Do not click on links that are embedded in unfamiliar emails. You can use your cursor to hover over the link and compare the actual URL with the displayed text without clicking on it.
- Do not open executable files (.exe / .scr / .cpl / .zip files) or Office documents that contain macros.
- Delete emails from services you don't use or from which you don't usually receive email, such as parcel services, banks, phone companies, or hotels.
- Ignore prompts to install software from an unknown source.

Keep your hardware and antivirus software up to date. Be careful with unknown apps.

- Internet-enabled devices should always be up to date.
- Install updates as they become available.
- Avoid downloading unknown apps to your hardware.

Do not accept every friend request on social media.

- Check whether you know the person and whether the request really is from that person.
- When in doubt, ignore the request.

Make only certain data and information accessible.

- Do not thoughtlessly disclose personal information.
- Please pay attention to which data you exchange inside and outside your company.

The first steps have been taken: You have defined clear responsibilities for cybersecurity in your organization, raised and reinforced awareness of the risks of cyberattacks among your workforce, and begun cultivating a cybersecurity culture.

Now it's time for Phase 2:

Phase 2
Take action and embed security

A **Embed cybersecurity within the organization**

B **Embed cybersecurity within products and services**

Phase 2 — A
Embed cybersecurity within the organization

Clear organizational measures are necessary to bolster cybersecurity in your own company. You should increasingly demand similar action from your business partners as well, referring them to the minimum requirements set forth in the Charter of Trust.

The internal measures to be taken and the external minimum requirements together provide a good orientation on how to best position your company. The emphasis is on topics such as data protection, security policies, responding to acute cybersecurity incidents, physical security, data integrity, access management, customer service, and training.

Learn more:

See the Charter of Trust website for more information on the 17 minimum requirements for suppliers:

www.charteroftrust.com


Integrity and availability
Data protection
Security policies
Site security
Minimum requirements
Support
Access, intervention, transfer & separation
Training
Incident response

Phase 2 — B
Embed cybersecurity within products and services

Companies that offer “smart,” network-enabled products and services are particularly vulnerable to cyberattacks and must meet the strictest requirements for their own cybersecurity – right from the start. After all, your products and services find their way directly into the infrastructure of your customers.

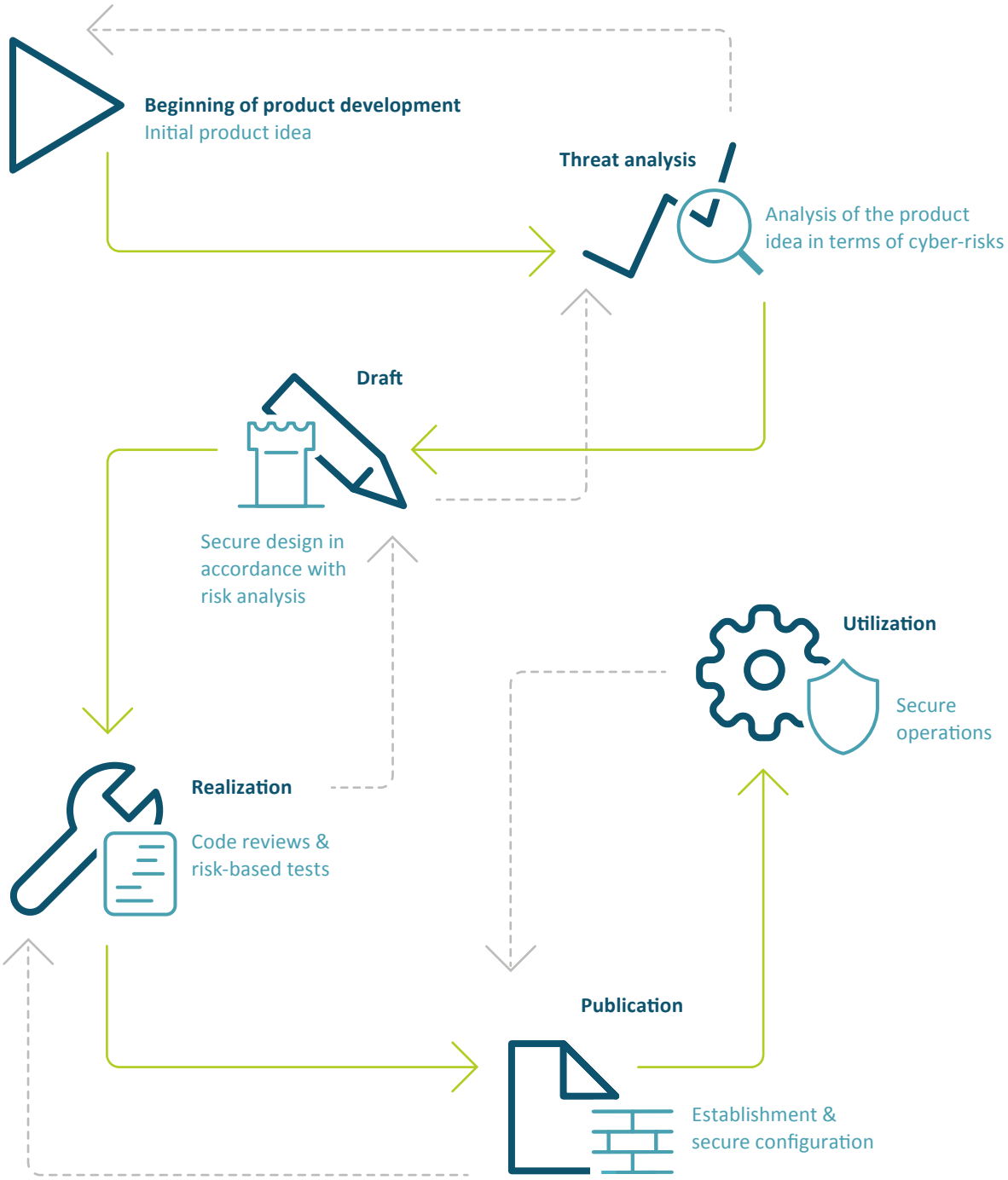
For this reason, your goal must be to implement effective cybersecurity measures across the entire product and service life cycle. This is known as “security by design.” The measures must be integrated into your existing processes: product management, research and development, project management, picking, operations, and service. The aim is to put the needs of your customers front and center. This is the only way to engender trust in your company.

Once you have integrated security by design into your processes, the next step will be to preconfigure your protective measures as a standard approach – security by default. You can learn more about security by design in the following section.

Learn more:

The website of the German Federal Office for Information Security (BSI) offers more information on “security by design”:

https://bit.ly/3atoUSa


Beginning of product development
Initial product idea
Threat analysis
Analysis of the product idea in terms of cyber-risks
Draft
Secure design in accordance with risk analysis
Utilization
Secure operations
Realization
Code reviews & risk-based tests
Publication
Establishment & secure configuration

Phase 2 of strategically positioning cybersecurity in your company was fairly extensive. But your company should now be well positioned against cyberattacks.

Now you should also consider the external impact of your measures. To remain competitive and demonstrate your strong cybersecurity stance to your customers, you should now – in Phase 3 – seek certification and work proactively to push for greater cybersecurity.

Phase 3
Make the structure of cybersecurity transparent, and be a role model for others

A **Publish your own cybersecurity setup**

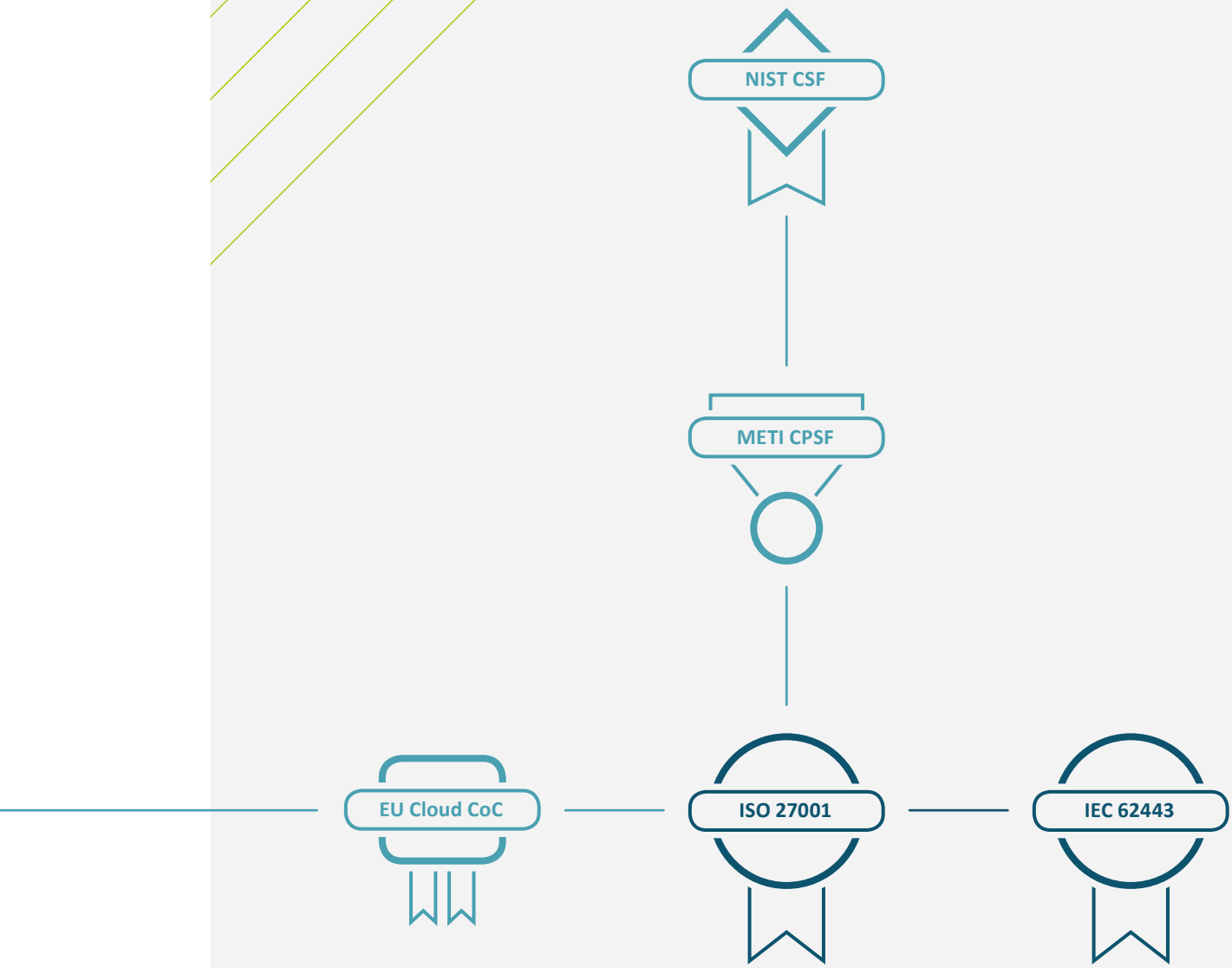
B **Become active – even outside your own company**

Phase 3 — A
Publish your own cybersecurity setup

Consider obtaining certification for your products and business processes

Demonstrate to your customers, suppliers, and partners that your company can deploy the best-possible arsenal to fend off cyberattacks, and have your products and solutions certified under such established standards as IEC 62443 or ISO 27001.

Complement this with regular security audits of your products, services, and solutions – for the protection of your partners and customers as well.



Learn more:

IEC 62443:
www.isasecure.org/en-US

ISO 27001:
www.iso.org/isoiec-27001-information-security.html

Phase 3 — B
Become active – even outside your own company

Take the initiative and boost collaboration on cybersecurity issues.

Cyberattacks do not typically stop at organizational boundaries or national borders. Quite the contrary: They can quickly escalate into a rapidly spreading threat. That's why it's important that solutions be found and implemented across organizational boundaries and national borders.

Use both new and existing forums to share cybersecurity information. With your stronger position in the area of cybersecurity, your company can serve as a role model for others and further strengthen itself through a robust exchange with the public sector, the scientific community, and trade associations.

Take advantage of your local chamber of industry and commerce for this type of exchange.

Charter for a secure digital world

At the Munich Security Conference in February 2018, Siemens and other global industrial companies launched a joint charter for more cybersecurity.

The Charter of Trust put forward 10 principles for better cybersecurity (see next page) that call on policymakers and businesses alike to take action. Because, as much as digital technology enriches our lives and fuels our economy, the risk of exposure to aggressive cyberattacks is also growing at an alarming rate. That's why we need to protect our economic, social, and democratic values from cyberthreats and hybrid cyberphysical threats.

To keep pace with rapid technological development and the threats posed by criminal elements, the public and private sectors need to pull together and focus their efforts. They must do everything they can to protect the data and assets of individuals and organizations; protect people, businesses, and infrastructures from harm; and create a reliable basis for trust in a digitally integrated world.

www.charteroftrust.com


aes
Allianz
Atos
BOSCH
DELL
Technologies
Deutsche Post DHL
Group
IBM
infineon
Microsoft
MITSUBISHI
HEAVY INDUSTRIES
msc
NTT
NXP
SGS
SIEMENS
TotalEnergies
TÜV
SÜD

Ten principles for a more secure digital world

01 **Ownership for cybersecurity and IT security**

Ownership for cybersecurity must be embedded at the highest levels of government through dedicated ministries and at the highest corporate levels through a chief information security officer (CISO). Clear measures and objectives need to be defined. And we want to establish the right mentality at all levels. Cybersecurity is everyone's job.

02 **Responsibility throughout the digital supply chain**

Businesses and, if necessary, governments must establish risk-based rules that ensure adequate protection across all levels of the Internet of Things, with clearly defined and binding requirements. Confidentiality, authenticity, integrity, and availability must be ensured through the definition of basic standards:

— **Identity and access management:** Networked devices must have secure identities and protection mechanisms that allow only authorized users and devices to access them.

— **Encryption:** Wherever necessary, networked devices must ensure confidentiality in the storage and transmission of data.

— **Continuous protection:** Companies must provide an appropriate framework for secure, automated updates, upgrades, and patches for their products, systems, and services.

03 **Security by default**

The highest appropriate level of security and data privacy must be applied, and this must be preconfigured when designing products, functionality, processes, technologies, operational workflows, architectures, and business models.

04 **User-centricity**

Companies provide products, systems, consulting, and services based on their customers' security needs and are available to them as trusted partners during an appropriate life cycle.

05 **Innovation and co-creation**
We must deepen the common understanding of cybersecurity requirements and rules between organizations and policymakers to continuously drive cybersecurity measures forward and adapt to new threats. Contractual public-private partnerships should be encouraged and supported. Industry-specific knowledge must be consolidated.

06 **Cybersecurity as a fixed component of education**
Special courses on cybersecurity must be integrated into curricula – as university subjects, in vocational education, and in training seminars – to push for the transformation of the required skills and career profiles of tomorrow.

07 **Cyber-resilience through conformity & certification**
Companies –and if necessary –governments ensure cyber-resilient products, systems, services and processes through conformity assessments including e.g., verification by independent parties.

08 **Transparency & Response**
Maintain and expand a network of experts who share new insights and information on incidents to foster collective cybersecurity;engage with regulators and other stakeholders on threat intelligence sharing policy and exchange best practices.

09 **Regulatory framework**
Multilateral cooperation in regulation and standardization must be promoted to create a level playing field for all stakeholders, akin to the global reach of the World Trade Organization (WTO). Cybersecurity rules should also be part of free trade agreements.

10 **Joint initiatives**
Joint initiatives with all relevant stakeholders need to be advanced to ensure prompt implementation of these principles throughout the digital sphere.

Publication information

Address Siemens AG
Werner-von-Siemens-Str. 1, 80333 Munich, Germany
Internet www.charteroftrust.com
Contact Phone: + 49 89 636 - 33443
Fax: + 49 89 636 - 30085
E-Mail: press@siemens.com

Text and editing Dr. Johannes von Karczewski, Kai Hermsen
Concept and design hw.design GmbH
Editorial office Dr. Renate Öttinger, Ingrid Tzschaschel
Print Gotteswinter und Aumaier GmbH

Sources (in German only)

[1-3] Bitkom e. V.: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie. Studienbericht 2018. https://bit.ly/2rFcGUW
[4] Bundesamt für Sicherheit in der Informationstechnik (BSI): Cyber-Sicherheit als Wettbewerbsvorteil in der Digitalisierung. https://bit.ly/2YHpRRf
[5-7] Bitkom e. V.: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie. Studienbericht 2018. https://bit.ly/2rFcGUW

How to respond to IT emergencies

Establish an emergency management protocol – written procedures and ad hoc measures – to be followed in the event of data theft, industrial espionage, or sabotage.

Stay calm and report the IT emergency

IT emergency number:

Who is reporting?

How did you work with the system? What did you observe?

Which system is affected?

When did the incident occur?

Where is the affected system located (building, room, workplace)?

Best practices

Stop working on the IT system

Write down observations

Take action only as instructed