Quality

Cybersecurity as a Matter of Competitive Advantage

Understanding cybersecurity as more than the sole fulfillment of regulatory requirements

Porsche Consulting
Strategic Vision. Smart Implementation.

INSIGHTS

//01

Cybersecurity is a growing matter of competitive advantage and goes far beyond the sole fulfillment of increasing regulatory requirements.

//02

A risk-based strategy, processes, organization and cultural awareness help maximizing cybersecurity while technology acts as a powerful enabler for the previous four levers.

//03

Top management must anticipate security trends and actively adopt to it, such as by collaborating with former foes (e.g., hackers) and by driving awareness (e.g., with attack simulations).

Introduction

Cyberattacks may take only seconds, but the recovery often takes months or even years and can cause significant business damage and reputational losses. The Norwegian aluminum company Norsk Hydro recently lost US $40 million due to multiple production stops caused by LockerGoga ransomware (Reuters, 2019). Roughly 50 GB of product construction and employee information were stolen from the automotive body manufacturer GEDIA after exposure to data theft (Handelsblatt, 2020). Moreover, not even government agencies are safe: in 2015, the German Parliament and numerous parliamentary office computers were infected by spy software, requiring the Parliament's IT system to be taken off-grid for several days, driving awareness for cybersecurity in Germany (Die Zeit, 2017). A 2020 study from Germany's Federal Office for Information Security showed the most common types of cyber incident as well as the average cost incurred per attack, as depicted in Figure 1. In addition, the current coronavirus pandemic is contributing to cyber risk as telework and online schooling become an integral part of our daily routines, requiring users to store and transfer sensitive data—thus providing hackers with new surfaces for attacks.

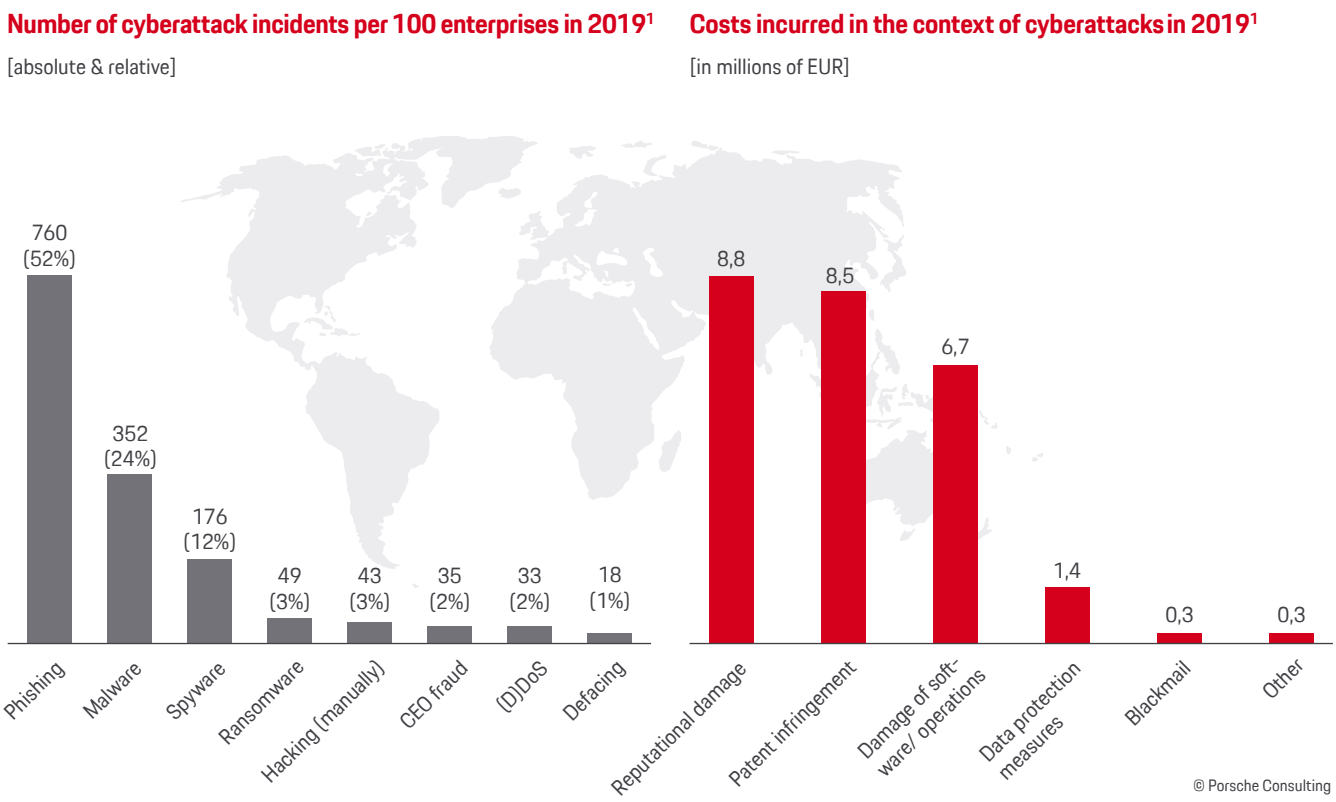


Figure 1. Cyberattack incidents by type and average cost per incident. Source: BSI, PWC & VHV Stiftung (2020)

Long story short: it's a good idea to be prepared for cyber risk.

Various stakeholders are paying increasing attention to whether a company is cyber secure or not: while customers trust companies to protect their personal information and patients do not want to be harmed while using IoT-enabled medical equipment such as pacemakers, investors do not wish to see production being cut off due to hacker attacks. Policymakers, however, are increasing pressure on companies to ensure cybersecurity as a means of consumer protection. Listening to such voices is important for companies that intend to make cybersecurity a competitive advantage, which aids at growing their (digital) business. But how exactly can cybersecurity offer a competitive advantage to businesses?

The answer is rather simple: while, for example, avoiding significant fines by protecting personal data is mandatory by regulation (e.g., General Data Protection Regulation threatens companies for data breaches with fines of up to 4% of global turnover; GDPR.eu, 2020), providing a secure product or service may become a unique selling point. Take the automotive industry: how about positioning your company as the most secure autonomous car brand worldwide? How about being the most secure financial transaction provider in your industry? Or would it not be desirable to make your healthcare company the number one in patient privacy? These examples show that in particular, companies whose brand builds around customer trust will benefit from positioning as cyber secure companies. The fact that by 2030, the average consumer will own ten connected devices, shows how much cybersecurity will become a winning argument across industries. The impact of this ever-increasing connectivity on cybersecurity becomes transparent by means of the automotive ecosystem as shown in Figure 2.

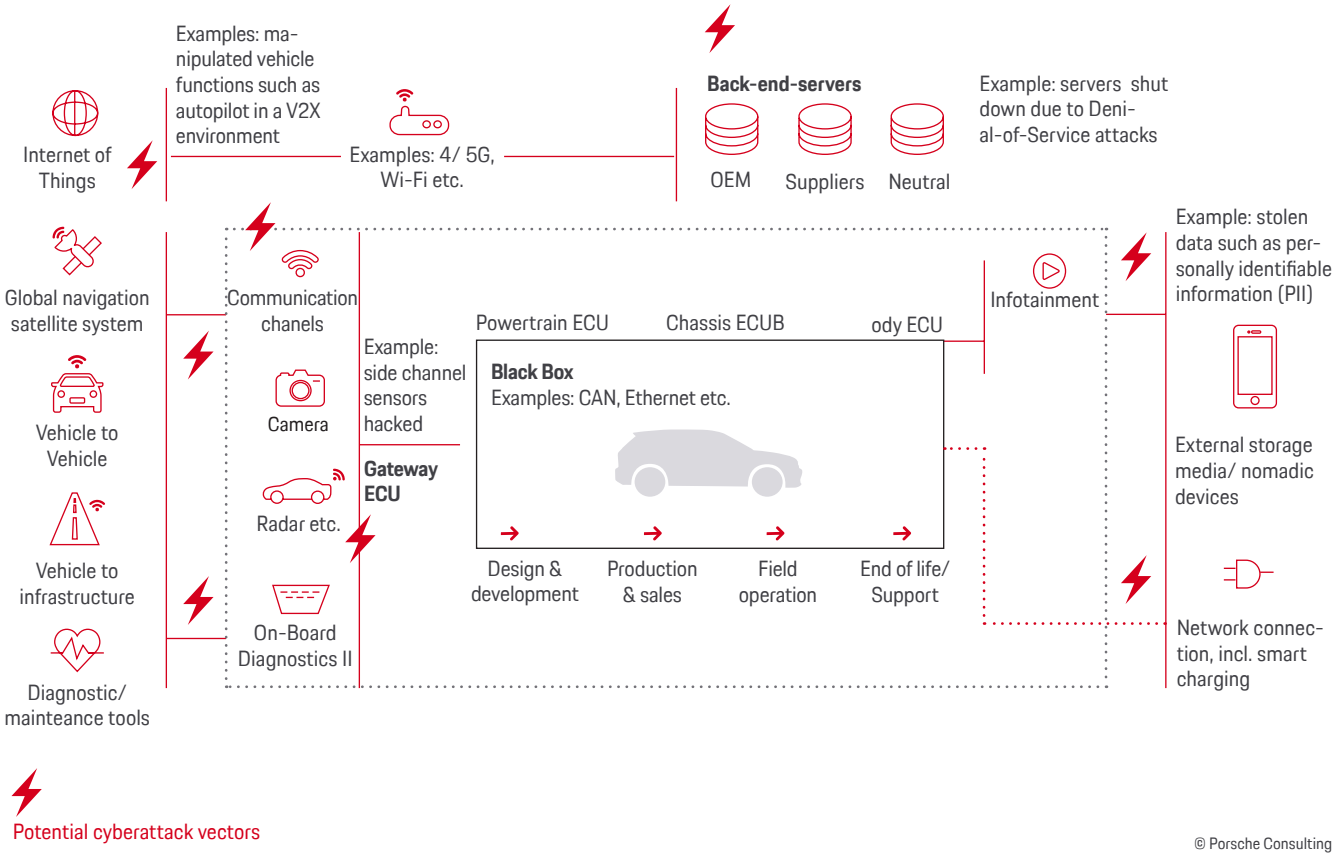


Figure 2. Attack vectors and resulting business risks in the product's ecosystem (example: a passenger car's ecosystem)

But instead of positioning themselves as cybersecurity leaders, most companies still struggle: 70% of German companies reported having suffered a cyberattack in 2017 (Federal Office for Information Security, 2018). Data breaches increased by 20% from 2018 to 2019 (Statista, 2020); in global terms, a monetary damage of cyberattacks of US $6 trillion is predicted for 2021 (Cyber Crime Report, 2020).

The good news is that four well-known levers may maximize a company's cybersecurity:

By **(1)** defining a risk-based cybersecurity strategy, companies are able to find the sweet spot between investing too many resources and building a resilient company.

(2) Cybersecurity processes will ensure that all relevant parties, such as development, quality, and IT, work closely together for one common purpose. The **(3)** cybersecurity organization will then be designed to ensure flexible and fast responses to any potential cyber risk. Finally, as cybersecurity is often a question of human failure, cultural awareness **(4)** is driven through focused communication and training. That is not to say technology doesn't matter—technology acts as a powerful enabler and will leverage competitive advantage if carefully integrated into the above-described levers.

- **However, let us first have a look at what is mandatory: regulation.**

01 | Fulfilling cybersecurity regulations is mandatory; going beyond is necessary

Ensuring effective cybersecurity should be more than a "check the box" exercise to meet regulatory requirements. A holistic view on this topic is required, as companies often set up cybersecurity without looking at the big picture, and lose their path on the way. Thus, adopting a cybersecurity framework such as that from the U.S. National Institute of Standards and Technology (NIST) or an industry-specific one, e.g., from the International Civil Aviation Organization (ICAO), is recommended as it supports the holistic view and ensures effective application of standards and best practices. The NIST framework, for instance, offers guidance on such topics as how to handle risk management, configuration, and vulnerability management, as well as cryptography.

One of the biggest challenges when coping with regulations is the fast pace of new cyber requirements coming into effect. Taking the automotive industry as an example, there are currently at least 18 standards relevant to vehicle type approval coming into effect by 2023—some of the most relevant are shown in Figure 3. Many companies already acknowledge this trend: some 88% of the companies asked gave growing regulatory requirements as a reason to invest in cybersecurity (Allianz, 2020). A failure to invest in cybersecurity may result in reputational damage, patent infringement, and damage of software or operations, to name a few of the most aggravating consequences.

For the automotive industry, implementing the new United Nations Regulation (UN-R) on Cybersecurity and Software Updates will be required as of 2022 (BMVI, 2020). A lack of certification for the required management systems according to the new regulation will result in the inability to further approve new vehicle types in more than 50 countries worldwide. The regulation requires automotive OEMs as well as

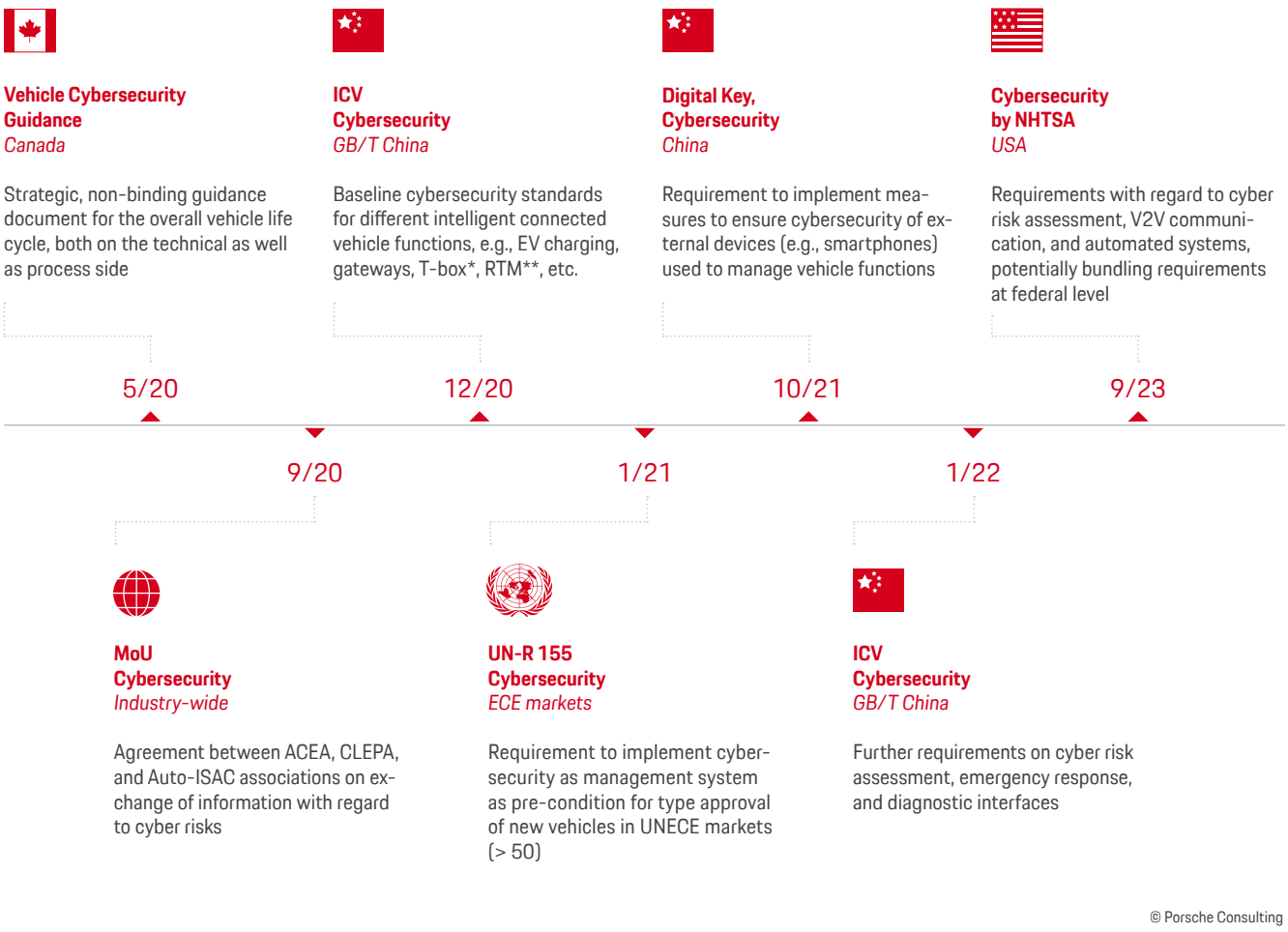


Figure 3. Main cybersecurity automotive regulations and standards coming into effect by 2023. (*connected-car standard terminal; **Real Time Monitoring)

suppliers to implement state-of-the-art cybersecurity and software update procedures. This applies throughout the product life cycle, i.e., for product development, production, all service, maintenance, and servicing after a component or software is commissioned. Thus, the entire automotive ecosystem (e.g., vehicles, connected devices, charging systems, servers, diagnostic/maintenance tools, etc.) is affected. Other industries, such as the medical device industry, are affected by increasing regulatory pressure too: in this industry alone, more than 25 guidance documents, including international standards for type approval, are currently in place (Porsche Consulting, 2020). Hence, the adoption of a strategic framework, including the above-mentioned levers, becomes imperative.

Furthermore, bear in mind that most cybersecurity regulations do not come with an exact implementation guideline. Instead, most regulations will simply offer mere requirements as a way to encourage companies to adopt individualized cybersecurity solutions, which are not easily exploitable by external parties. In other words, be prepared to spend time on carefully interpreting regulation. A systematic, cross-industry approach to translating regulation into tangible outputs and measures for companies is shown in Figure 4. This checklist approach integrates cybersecurity best practices according to four main categories of regulations and standards (Prevent, Detect, Defend, and Update) that are relevant to any industry. Thus, using this approach reduces the time needed to interpret and ramp up for regulation fulfillment.

Nr.	Category	Requirement	Requirement Description	Regulatory Market Requirements Reference	Standards Reference (ISO/IEC/AAMI etc.)	Coverage Check	Mitigation Code	Prioritized Mitigation
1	**Prevent**	Limit Access to Trusted Users & Devices Only	**Limit Access to Trusted Users & Devices Only** (follow sub requirements)	**China** (e.g., GB/T)	**NIST**	**2**	*N/A*	*N/A*
1.1	Prevent	Limit Access to Trusted Users & Devices Only	-Limit access to devices through the authentication of users (e.g., user ID and password, smartcard, biometric).	**China** (e.g., GB/T)	**NISTIEC 60601(series)**	**2**	*A1*	*Implement user authentication for client (end-user) to restrict access to medical device for unauthorized users (User-friendly authentication (e.g. password authentic.)*
1.2	Prevent	Limit Access to Trusted Users & Devices Only	-Use automatic timed methods to terminate sessions within the system where appropriate for the use environment	**USA** (e.g., FDA)	**NISTIEC 60601(series)**	**4**	*not relevant*	
2	**Detect**	Detect and Log Events	Implement design features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use	**EU** (e.g., MDR)	**ISO13485(series)**	**1**	*A3*	*Ensure detection systems on medical device (Intrusion detection system (e.g. antivirus scan)*
3	**Defend**	Communicate to Customers	Notify users upon detection of a potential cybersecurity breach	**USA** (e.g., FDA)	**IEC 62304(series)**	**4**	*N/A*	*N/A*

Systematization of requirements | **Translation of requirements into tangible outputs and measures** | **Reference to further standards/regulations** | **Statustracking**

Figure 4. Cross-industrial regulatory requirements checklist according to processes (protect/detect/defend). Source: Porsche Consulting Tool/Recherche

And last but not least: accept the residual cyber risk. No solution will ever cover all possible outcomes. The challenge is to reduce occurrence probability to a minimum and mitigate the potential impact of those risks an organization simply cannot cover. In any case, restricting cybersecurity to regulatory requirements does not seem to be an expedient, holistic approach. One should understand cybersecurity as an opportunity to create a competitive advantage rather than as an unavoidable evil.

02 | Meeting well-known levers: strategy, processes, organization, and cultural awareness

After understanding the regulatory requirements specific to an industry, the above-mentioned four levers strategy, processes, organization, and culture should be adjusted to the company's needs to foster cybersecurity. How does this work?

2.1 ADOPTING A CYBER RISK-BASED STRATEGY

Strategic decisions highly affect the approach to become cyber secure. As a starting point, one should analyze whether cybersecurity might offer any competitive advantage for the specific business, which means knowing the respective business cyber risk profile. We define business cyber risk as the sum of financial and reputational loss a company might incur in case of cyberattacks to its products.

Figure 5 offers guidance on which might be a product's and business model's cyber risk profile. For this exercise, consider two relevant dimensions (x- and y-axis) for the assessment: the y-axis describes the risk level that a company might face if data were stolen or corrupted, which would mean a potential violation of privacy and/or loss of corporate knowledge. Ideal targets for hackers include online banking systems or educational platforms with a high inherent degree of privacy and knowledge risk. On the other hand, the x-axis describes the risk that a company must consider if a cyberattack would lead to a loss of product functionality or even harm customers physically. The latter risk is especially pertinent to the medical device industry. Such is the case for surgical robots or implanted devices (e.g., pacemakers), as patient safety is a priority here.

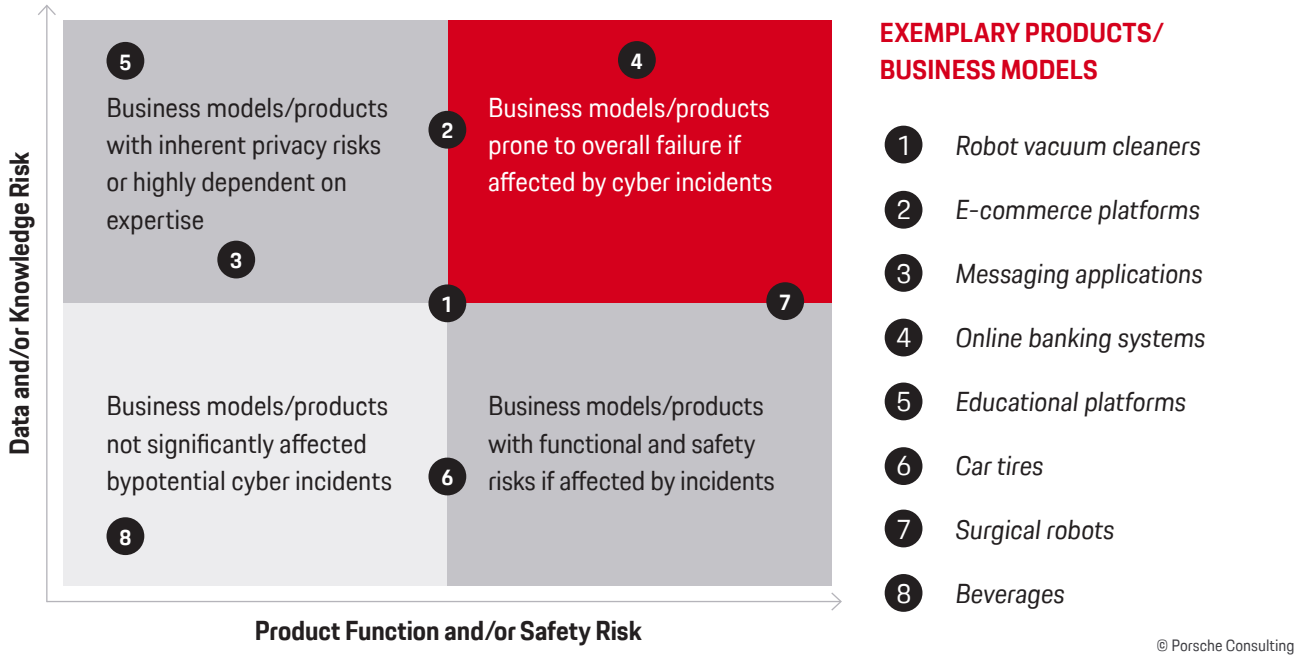


Figure 5. Product/business model risk matrix including diverse examples.

Therefore, if data privacy at your company is non-critical, and unsecured products will not put the safety of your customers at risk, or if you simply do not supply a connected product, you will not want to invest double digits in cybersecurity. This is often the case for companies and industries primarily focused on hardware products with no software or very little involved (e.g., tire manufacturers), or if you act at the very beginning of a value chain (e.g., raw material suppliers such as for steel). What is important is that you know your business cyber risk profile before making investment decisions and that you carefully check whether cybersecurity might be a relevant competitive advantage to your company.

After ascertaining if cybersecurity bears a risk for your business, decide whether to externalize or internalize cybersecurity. This is important because internalizing will require your company to invest and build up internal expertise, which might take time to do and which reduces flexibility. Whether, for example, you opt for a software as a service (SaaS) or an on-premise solution will significantly affect the level of required resources. While a SaaS solution will provide full external cloud management and high flexibility to your company, an on-premise solution will require you to contract highly trained personnel and invest in your own cybersecurity infrastructure. Thus, finding the sweet spot between being able to manage your own cybersecurity and limiting your budgets becomes a fundamental decision to make. Again, keep your cyber risk profile in mind when making this decision.

Third, based on your risk profile, consider the impact of some of the following levers. For example, decide on what organizational level to anchor your cybersecurity decision-making. A higher cyber risk profile might make short-timed decision-making highly relevant. It might also imply that regulation obligates you to nominate a person responsible for cybersecurity in your company, such as a chief information security officer (CISO). In this case, making cybersecurity part of the top management agenda and committees is a good idea. Another example includes the decision on whom to cooperate with on cybersecurity, as most companies struggle to build up internal expertise. Collaboration with former foes, such as hacker groups, or universities, might make sense for many companies. Refer to Section 03 for further details on new types of collaboration.

2.2 DESIGNING CROSS-FUNCTIONAL CYBERSECURITY PROCESSES

Strategy is the backbone of a successful cybersecurity assurance. But strategy will not succeed if not translated into processes that ensure end-to-end collaboration of all relevant parties for ensuring cybersecurity such as the development, quality, IT, and customer service departments. Thus, we propose embedding four types of core processes into a company's process landscape over the whole product life cycle as shown in Figure 6: preventive, detective, defensive, and updating processes. Technology, as mentioned in the introduction, acts as an enabler for these processes.

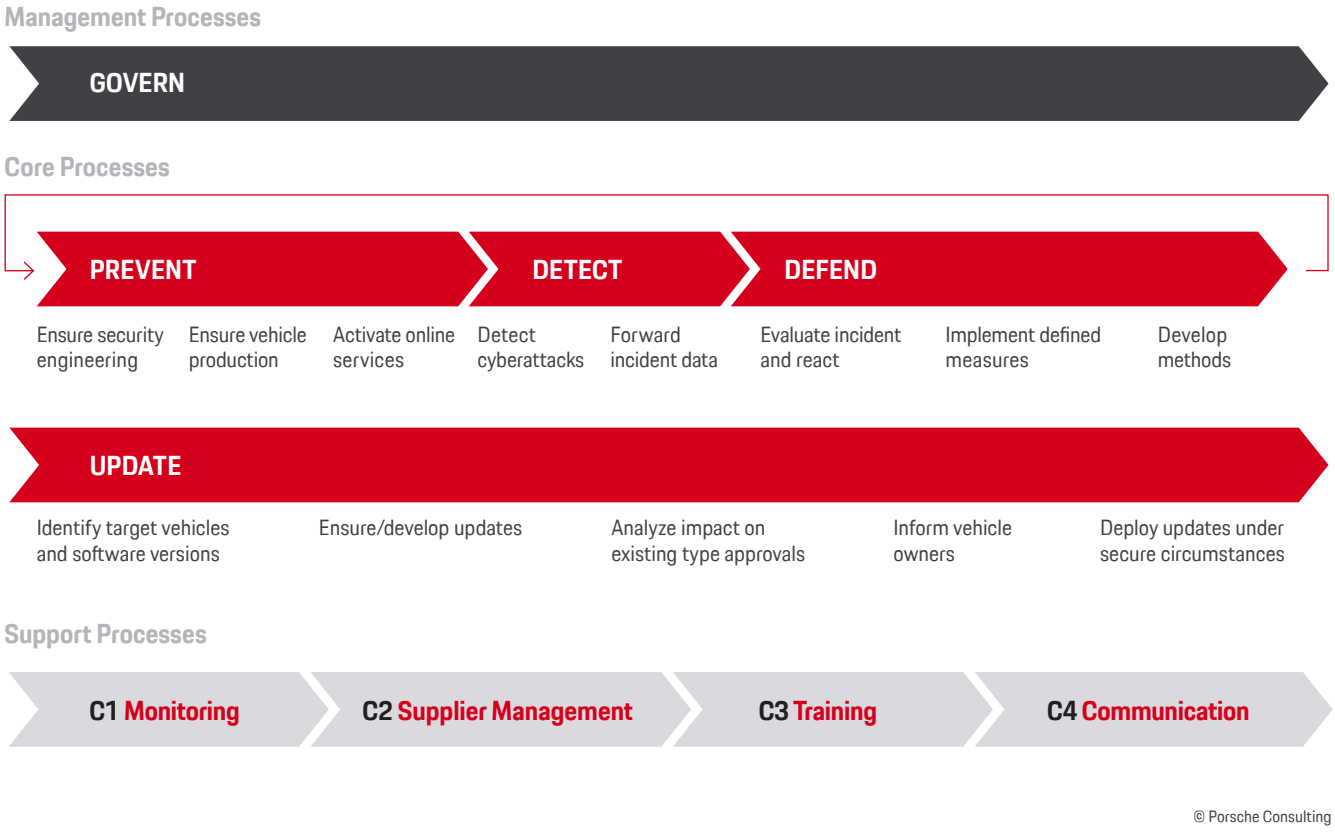


Figure 6. Exemplary cybersecurity management, core, and support process model.

Preventive processes will focus on deeply integrating security into a product while still in development—this is known as the "secure by design" approach. Reducing the attack surface, achieved by hardening software code, deactivating useless functions, or updating systems, is imperative in this phase. Technologically, this may be enabled by employing multi-factor authentication and cryptographic techniques to prevent unauthorized access to critical systems and/or data. Collaboration between development and IT departments is crucial in this process, especially when it comes to integrating cybersecurity requirements into the system or other procedures such as penetration testing.

Next, **detective processes** will help to anticipate cyber risks while products are in use. Two aspects are relevant to detection: first, checking for vulnerabilities, i.e., potential attack vectors not yet sufficiently accounted for; and second, checking for actual intrusions. Standardizing the reaction through processes with the right degree of flexibility aids in effectively averting greater damage fast.

Data-driven monitoring such as provided by many intrusion detection systems may help to prevent and/or detect attacks on time-based methods such as pattern or signature-based recognition. Often, it is at this stage that collaboration between field observation, development, and customer service departments becomes crucial. While field observation ensures rapid detection, development will provide a solution such as a software update, and customer service delivers communication that is specifically targeted to clients.

Finally, **defensive and update processes** will enable reaction to potential intrusions. The defensive process ensures recovery and triggers the update process that brings bugs and unwanted security breaches to an end. Intrusion detection systems, as described above, may include functions that not only detect but also defend from a potential intrusion. Typical defense measures include shutting off or isolating critical system partitions, blocking, or redirecting harmful incoming data. Again, cross-functional work is necessary.

2.3 BUILDING A SUITABLE ORGANIZATION

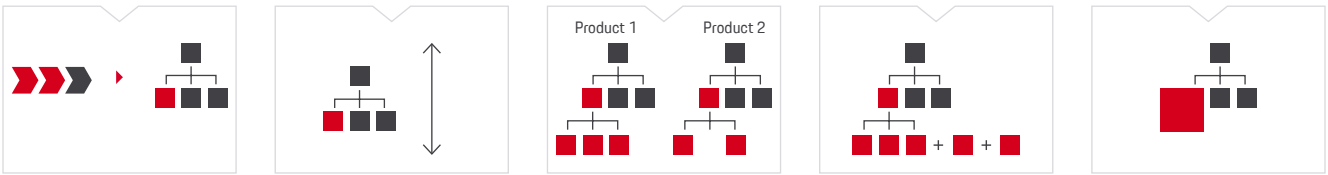
As processes drive organizational structures, the latter need to enable flexibility and fast response times while effectively avoiding intrusions and limiting the extent of potential damage.

Companies often struggle while defining a suitable organizational design, as cybersecurity appears as a relatively new topic, especially product-oriented security. Companies need to consider five criteria as shown in Figure 7, which aid in defining a cybersecurity organizational structure.

The organizational structure for cybersecurity organization may be build based on five main criteria:

Security Organization | Organizational design criteria (excerpt)

01	02	03	04	05
Depth of added value	**Cyber risk severity**	**Product substance**	**Market requirements**	**Growth strategy**
R&D, production, and sales of IoT enabled-products	Impact on product safety (e.g., inadvertently harming customers' health)	Homogeneous product portfolio and similar CS2 requirements (e.g., EA[3])	Comparable requirements in markets (e.g. standardized type approval in aviation)	Increase of product portfolio (e.g. release of new IoT services)
Development only for IoT-enabled products (e.g., security by design)	Impact on data privacy (e.g., loss of customer data)	Heterogeneous product portfolio and similar CS[2] requirements (e.g. EA[3])	Specific requirements in markets (e.g., type approval for medical devices)	Market expansion (hence, facing new market specific requirements)
Production only for IoT-enabled products (e.g., CoP[1])	Impact on finance and operations (e.g., critical financial services)	Heterogeneous product portfolio and differing CS[2] requirements (e.g. EA[3])	Mixture of market requirements due to cross-industrial product divisions	Organizational growth (hence, tailoring enterprise security)
Organizational and processual structure	Organizational hierarchy	Organizational anchoring in product/functional departments	Department specific splits (e.g., sub-departments)	Size/scaling of departments



1 CoP = Conformity of Production | 2 CS = Cybersecurity | 3 = Electronic Architecture

Figure 7. General organizational design criteria for cybersecurity.

Apart from the company's cyber risk profile, which, again, is important to consider, take the impact of the depth of value added (01) as an example: whether a company develops, produces, or just markets a product will define in which departments cybersecurity structures are required. A contract manufacturer, for instance, will not need to build up cybersecurity detection capabilities.

Another example is product substance homogeneity: as electronic architectures differ among products, different attack vectors need to be covered. This will strongly affect the degree to which cybersecurity structures are centralized into one single functional department, or decentralized according to your product structure.

In any case, make sure to always bear your strategy and process landscape in mind while designing your cybersecurity organization, unless you are looking for an organization unable to deliver the results you wish. For further insights on organizational design, refer to our white paper "The Quality Organization of the Future" on porsche-consulting.com.

2.4 DRIVING CULTURAL AWARENESS

While only 3% of all cyberattacks are due to sophisticated hacking, an astonishing 52% are caused by standardized (e-mail) phishing and ransomware attacks that are human-induced security breaches (BSI, PWC & VHV Stiftung, 2020; cf. Figure 1). Further, newer forms of cyberattacks such as social engineering bots that fake personal identities contribute to an environment in which attacks are increasingly harder to identify. On top of that, the intangibility of software makes the risk less visible. While in the case of hardware, it is easy to talk about the look and feel or the robustness without being an expert, this is no longer the case with cybersecurity. In addition, the stress caused by an intrusion attempt might do the rest of the job—by avoiding an adequate response. That is, no strategy or process will do the job if employees are not aware of cyber risk. Aware employees will recognize characteristics of intrusion attempts and respond effectively. So how can cultural awareness of cybersecurity be fostered?

A newer method to foster cultural awareness is the use of cyberattack simulations. These simulations may range from company-wide mailings that include links to apparently unsecure websites (instead explaining the risks of unsecure links) to executive-level cyber simulations such as depicted in Figure 8. In the latter case, the participants plunge into a full simulation of a cyberattack and play out their reaction. As such, the simulation covers all procedural aspects, beginning with the detection of an attack, continuing with its defense, and finally recovery. Such simulations will not only drive awareness for cyber risks, but also provide an understanding about potential areas of improvement. Make sure to bear some success factors in mind: involve all relevant departments and top management, as cybersecurity is a cross-functional and -hierarchical exercise. Create a scenario

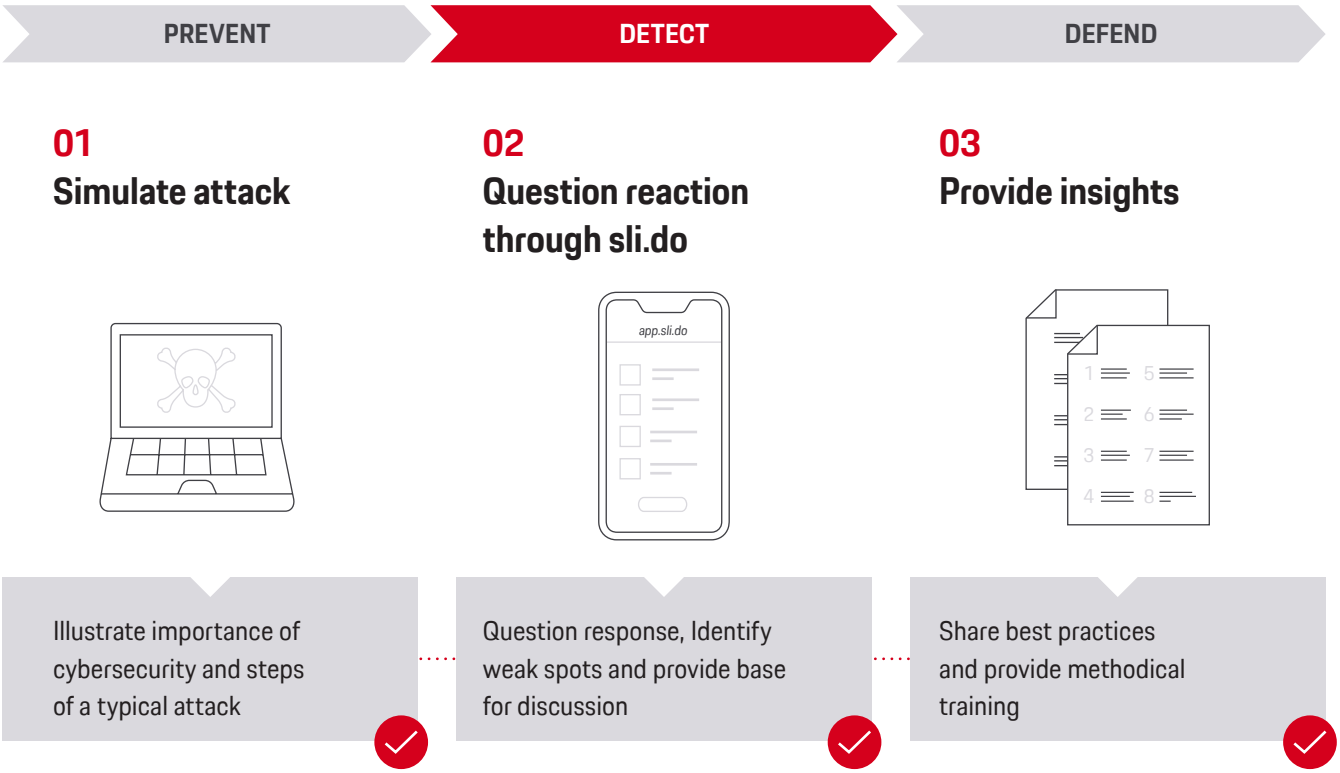


Figure 8. Benefits of a cyberattack simulation.

that is as realistic as possible, as this will drive up the stress level. After the simulation, follow up on the identified areas of improvement and materialize them into a concrete plan of action.

At its best, these simulations should be embedded into a company-wide training and communication plan. Since "culture eats strategy for breakfast" (Peter Drucker), make sure to drive further awareness with focused communication measures such as a clear tone-from-the-top message that encourages employees. At the same time, deliver target-specific training and replace the one-and-done training model with short, repetitive and engaging modules spread out throughout the year. In addition, reporting of potential loopholes should be encouraged and made as easy as possible. This will help to fill processual gaps, as not everything will be (or should be) covered by a fine-grained process. Consequently, by building a cybersecurity cultural awareness, every single employee will become a member of the security team.

03 | What happens next in cybersecurity?

In the fast-evolving cybersecurity environment, companies should prioritize anticipating trends and risks. By anticipating risk, companies can prepare on time and foster cybersecurity as a competitive advantage. So what topics should be on the top management agenda?

- **Cooperate—especially on technology:** As defensive capabilities advance, as is the case with, for example highly automated and machine learning systems, attackers are becoming more sophisticated too. In order to keep ahead of the game, most companies—especially small and medium-sized businesses—will struggle to build up expertise at the required pace. Cooperation with third parties becomes mandatory. Potential cooperation partners include universities, cyber risk-specialized companies for penetration testing or even former foes, commonly known as hackers. Companies such as Tesla are actively taking advantage of the expertise of the latter, promoting its "Hall of Fame" for those hackers identifying the most relevant security vulnerabilities (Zero Day Initiative, 2020). In any case, third parties should support the outside in view to keep up the pace.

- **Manage the skill gap:** The cybersecurity workforce needs to grow by 145% to meet the global demand for skilled professionals (ISC, 2019). Besides appropriate education and training, closing this gap also links back to cultural aspects. Create a culture that cybersecurity experts will want to be part of—Generation Z being the focus group, as they are most likely equipped with a digital mindset. Offer them a clear cybersecurity career path and allow for diversity.

- **Protect critical data:** In an era where data and information has never been as important as today, be sure to protect them. These data may include corporate knowledge or personal customer data such as private health records or payment information, since both can be worth a fortune on the black market (John Shin, 2019). Fines due to breaches of the General Data Protection Regulation may go up to 4% of the company's annual turnover (GDPR.eu, 2020). They are expected to further increase, as the examples of data breaches at British Airways (£20 million; ICO, 2020a) and Marriott (£18.4 million; ICO, 2020b) show. Make sure to segregate and encrypt critical data.

- **Consider the whole chain:** A company may be resilient to cyber risk. Yet is the same resilience ensured along the entire value chain that the company depends on? In terms of computer networks, this question applies to partners along the whole value chain, such as tier 1 and tier 2 suppliers, as well as to the "man in the middle." It is important to require all partners on all ends of the chain to comply, be cyber secure, and to provide proof of it.

To sum up, company leaders and management should keep in mind the words of Joachim Müller, CEO of Allianz Global, Corporate & Specialty, when approaching the topic of cybersecurity:

"Preparing and planning for cyber risks is both a matter of competitive advantage and business resilience in the era of digitalization." (Allianz, 2020).

Key questions managers need to ask

- Do I know my company's cyber risk profile and do I have a clear picture of the effect on my company's competitive advantage in the event of a cyber threat?
- What do my cybersecurity measures and structures look like in terms of protecting my company, products, customers, and other third parties? How fast and efficiently could my company respond?
- Am I certain to comply with all cybersecurity regulations and standards that are relevant to my company and its products? What is my remaining exposure to cyber threats after complying?
- How have I anchored cybersecurity into my company? What can I do to foster cybersecurity awareness? Are the right kind of enablers in place?
- Do I have cybersecurity measures and structures set and prepared for that allow and foster cross-functional and -hierarchical work?
- Do I already have the right set of skills on my team? If not, whom do I train to have which kind of skillset? Which external partners should I collaborate with?
- Am I aware of relevant future cybersecurity trends that could have an impact on my company?

IN BRIEF

01 Cybersecurity is becoming a matter of competitive advantage for companies due to increasing connectivity and pressure from diverse stakeholders such as customers and policymakers.

02 Preparing for cybersecurity requires the adoption of a holistic framework/management system, which allows for cross-functional and -hierarchical collaboration.

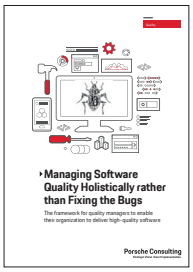
03 A holistic approach to cybersecurity is achieved through aligning four well-known levers: strategy, processes, organization, and culture with technology as enabler.

04 Being cyber secure means covering the whole life cycle - from building in preventive protection into your products' and company's ecosystems, to effectively detecting and responding to potential intrusions through covering vulnerabilities by updating routines.

05 As cybersecurity is people-driven, ensure cultural awareness by adopting new methods of training and communication, such as a cybersecurity attack simulation.

06 Keep up the pace with new trends in order to anticipate cyber risk, such as the lack of a qualified workforce.

Further reading



Managing Software Quality Holistically rather than Fixing the Bugs

The Quality Organization of the Future

Porsche Consulting INSIGHTS

Authors

Oliver Stahl
Associate Partner

Roman Baecker
Senior Manager

Dr.-Ing. Michael Bartholdt
Senior Consultant

Sebastian Roth
Senior Consultant

Arber Sejdiu
Senior Consultant

Contact
+49 170 911 4330
oliver.stahl@
porsche-consulting.de

Porsche Consulting

Porsche Consulting GmbH is a leading German strategy and operations consultancy and employs 670 people worldwide. The company is a subsidiary of the sports car manufacturer Dr. Ing. h.c. F. Porsche AG, Stuttgart. Porsche Consulting has offices in Stuttgart, Hamburg, Munich, Berlin, Frankfurt am Main, Milan, Paris, São Paulo, Shanghai, Beijing, Atlanta, and Palo Alto. Following the principle of "Strategic vision. Smart implementation", its consultants advise industry leaders on strategy, innovation, performance improvement, and sustainability. Porsche Consulting's network of 12 offices worldwide serves clients in the mobility, industrial goods, consumer goods, and financial services sectors.

Appendix

References

(1) *https://de.reuters.com/article/norway-cyber/norsk-hydro-details-loss-from-cyber-attack-says-aig-lead-insurer-idUSL8N21D3WX*

(2) *https://www.handelsblatt.com/unternehmen/industrie/autobranche-hacker-erpressen-wichtigen-zulieferer-autokonzerne-koennten-auch-betroffen-sein/25469710.html*

(3) *https://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia?utm_referrer=https%3A%2F%2Fwww.google.com%2F*

(4) *https://kfn.de/wp-content/uploads/Forschungsberichte/FB_152.pdf*

(5) *https://gdpr.eu/gdpr-fines-so-far/*

(6) *Porsche Consulting based on Kai-Frederik Zastrow as published here: http://www.oica.net/wp-content/uploads/The-future-UN-Regulations-on-Cybersecurity-and-SW-updates-PSA-Group-Kai-Frederik-ZASTROW.pdf*

(7) *https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf?__blob=publicationFile&v=3*

(8) *https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/*

(9) *https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf*

(10) *https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/Allianz-Risk-Barometer-2020-press-release_EN.pdf*

(11) *https://www.bmvi.de/SharedDocs/DE/Artikel/StV/Strassenverkehr/un-ece-regelungen.html*

(12) *https://kfn.de/wp-content/uploads/Forschungsberichte/FB_152.pdf*

(13) *https://www.der-bank-blog.de/peter-drucker-ueber-unternehmenskultur-und-strategie/zitate/13830/*

(14) *https://electrek.co/2020/01/10/tesla-hacking-challenge/*

(15) *https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study*

(16) *https://www.disruptordaily.com/cybersecurity-technology-trends/*

(17) *https://gdpr.eu/gdpr-fines-so-far/*

(18) *https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/*

(19) *https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/*

(20) *https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/Allianz-Risk-Barometer-2020-press-release_EN.pdf*

Porsche Consulting

Stuttgart | Hamburg | Munich | Berlin | Frankfurt am Main | Milan | Paris | São Paulo | Atlanta | Palo Alto | Beijing| Shanghai

www.porsche-consulting.com