ICT, Strategy & Policy
www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO 2025 R11540 – 1st of August

Cybersecurity by design

Investigating the drivers and barriers for the adoption of cybersecurity by design

Author(s)	Rick Gilsing Alexandra Garban Vera Irmak Thomas Rooijakkers

Classification report	TNO Public
Title	TNO Public
Report text	TNO Public
Number of pages	19
Number of appendices	0

All rights reserved
No part of this publication may be reproduced and/or published by print, photoprint, microfilm or any other means without the previous written consent of TNO.

© 2025 TNO

Contents

1 Introduction

In today's world, businesses, governments and people are operating in a highly digitalised society. Over the past two decades, we have seen digital transformation taking place in different facets of our modern society, with digital solutions and services becoming part of regular business operations and our day-to-day activities. For example, modern workspaces in organisations have frequently become virtual spaces, in which employees communicate and collaborate with each other largely through digital means. Communication services such as Microsoft Teams, Zoom or Slack enable organisations to bridge the physical gap between its employees and to help them to work together. Similarly, to support the integration of various business units and functions, organisations generally are built and reliant upon digital, integrated management systems that help them coordinate cross-functional (and often even cross-organisational) actions. As a result, examples of such management systems such as SAP and Oracle are well-known and widely adopted by contemporary organisations to help them in doing so. Lastly, we also see that products and solutions are increasingly becoming digitalised, with organisations seeking to offer additional sources of value creation to customers by offering products that are able to connect and interact to existing digital ecosystems. Traditionally 'mundane' goods such as TVs, sound installations, lighting and appliances more typically include connectivity features to create interconnected systems for additional value creation.

Evidently, this digitalisation trend means that we are operating in a largely virtual and interconnected world. (Sensitive) information is generated, collected and shared through products, systems and systems-of-systems, and can as such be authorised for access and use at different points in the ecosystem. Similarly, products and services can be interacted with through digital infrastructures accessible at different locations. Whilst the merits of this virtual world are clear, this transition also stresses the importance of ensuring that the ecosystems we create are robust and secure. Accordingly, realising **cybersecurity** – the protection of cyber-based or cyber-supported systems from internal and external threats to ensure continuity and security – should go hand in hand with this digital transition. More and more, we see examples of cases justifying the need to focus on cybersecurity when developing new products and services. Cybercriminals are leveraging techniques such as ransomware attacks, phishing attempts, exploiting data leaks or bypassing security systems to gain access to sensitive information or control products and systems remotely without consent of the owners. Without (continuously) up-to-date cybersecurity, such products become easy targets for criminals. In addition, the need for cybersecurity can also demonstrate itself from non-malicious events. For example, the *Crowdstrike* incident in 2024, caused by erroneous patches for security software used in many Windows-based products and services, resulted in the outage of roughly 8.5 million systems worldwide for a duration of time; its impact could have been decreased through the integration and adoption of cybersecure principles.

Despite the examples above, we discern that organisations do not always consider cybersecurity by design when manufacturing new products or services. Often, organisations are reactive in how they approach cybersecurity, improving security principles and protocols for new products *when* impactful events occur (for example when competitors are victim of a cyber-attack), or *if the* market forces organisations to adhere to new security principles. One explanation for this could be the fact that cybersecurity, in principle, creates value by reducing

or preventing risks as a result of cyberthreats and resilience. However, as such threats are uncertain and may not necessarily occur, the value of cybersecurity may be difficult to articulate, leading organisations to focus on different aspects related to product development instead.

Nonetheless, it would be valuable to understand what is hindering organisations to embrace cybersecurity by design. If identified barriers can be addressed, resolved, or removed, this can pave the way for organisations to increase their maturity in terms of realising cybersecurity by design. Additionally, it would also be valuable to understand what is fostering organisations to enable cybersecurity by design. Such key antecedents or best practices could offer a fertile ground for organisations to become more mature and could help to guide organisations in innovating their current product development and business processes towards those that instil cybersecurity by design.

In this report, we aim to unveil these barriers, drivers, challenges and opportunities for organisations towards realising cybersecurity by design, with a specific interest in the drivers and barriers for organisations that deal with the development of cyber-physical products and systems. Such organisations are currently transitioning from purely physical products towards products that feature digital services and solutions and hence are experiencing the barriers and drivers for cybersecurity as we speak. In addition, we complement these insights to organisations which already have built up maturity in terms of cybersecurity by design to understand potential best practices that can be used. Accordingly, we pose the following research objective:

"What barriers, drivers, challenges and opportunities towards realising cybersecurity by design can be identified for organisations?"

Through a series of semi-structured interviews, we present preliminary findings obtained from eight organisations on the role of cybersecurity for them and the actions they have taken to enable cybersecurity by design. We also communicate on what is driving but also hindering organisations to do so. Based on these preliminary findings, we propose a set of best practices that organisations may consider or reflect upon to foster cybersecurity by design.

This report is structured as follows:

Section 2 describes the research approach followed, explaining the set-up for the research as well as the protocol adopted;

Section 3 describes the results of the research, listing the common barriers and drivers identified through the interviews;

Section 4 lists the best practices and key aways to consider as part of the research;

Section 5 concludes this report and presents the next steps to be taken;

2 Research approach

In this section, we detail the research approach followed to provide answers to our research question. Figure 1 presents an overview of the research approach and the steps taken. In the following, we detail each of these steps.

Figure 1: Research approached followed, including the steps 1) investigation of the SotA literature, 2) elicitation of insights from industry experts and 3) analysis and sensemaking.

2.1 Investigation of state-of-the-art literature

Step 1 concerned an investigation of the state-of-the-art literature on the barriers and drivers towards the adoption of cybersecurity (with a specific interest on how this can be enabled 'by design').The goal of this step was twofold: on the one hand, this step helped to unveil important barriers and drivers already identified towards the adoption of cybersecurity, and to understand what potential gaps might still remain in light of adoption of cybersecurity by design. On the other hand, the literature search also helped us to develop an interview protocol to elicit insights and best practices from industry experts, building upon the barriers and drivers identified in literature.

To identify relevant publications and works on the adoption of cybersecurity in practice, we relied on academic libraries such as Google Scholar, Web of Knowledge and Elsevier. To support and structure our search efforts, we applied a keyword-based protocol, for which the following search string was used:

"cybersecurity" AND "adoption" AND ("drivers" OR "incentives" OR "barriers" or "challenges")

Accordingly, for the publication to be considered relevant, we considered that any publication should take both 'cybersecurity' and 'adoption' into account as part of their core. In addition, we posed that relevant publications should discuss either drivers, incentives, barriers or challenges (which are often used synonymously) in light of the adoption of cybersecurity. Since negative drivers can be considered barriers (whereas positive challenges can potentially lead to being a driver or incentive), we did not impose that relevant publications should necessarily consider all aspects simultaneously.

Through our keyword search, we identified a large set of potentially relevant publications, for which we then analysed the title, and (if relevant) abstract of each publication. Based on this, we removed any publications which seemingly did not fit our research question. For example,

some publications in our preliminary set focus on cybersecure information sharing. Whilst this can be related to (adoption barriers and drivers for) cybersecurity embedded for products and systems of organisations, it concerns a different topic of interest. Accordingly, such publications were considered out of scope for our research and removed.

We further scanned the remaining set of publications to identify what barriers, drivers, incentives and / or challenges were described. In parallel, we created a longlist to keep track of what barriers, drivers, incentives and / or challenges were already mentioned as well as their frequency. Once we felt confident that the list was saturated – i.e., through reading additional publications no new barriers, drivers, incentives and / or challenges were identified – we stopped our search efforts. We then further detailed each barrier, driver, incentive and / or challenge listed and assessed how these were interpreted by the publications included. We also studied the set of publications to identify potential gaps or directions for future research to take into account for our interviews.

2.2 Elicit insights from industry experts

As per **Step 2,** to generate answers to our research objective, we conducted 10 semi-structured interviews with stakeholders at organisations dealing with cybersecure solutions or challenges in April – June 2025. In light of our research objective, we focused on organisations that deal with cybersecurity in products, systems or systems-of-systems. Accordingly, such organisations can be providers of cybersecure solutions, service providers on cybersecurity or deal with cybersecurity as part of their day-to-day operations. The latter calls for a more explicit focus on high-tech manufacturing or servicing in which cybersecurity challenges tend to be more pervasive. In terms of respondents, we looked for interviewees which were 1) working with cybersecurity on a regular basis and / or 2) were able to communicate in a broad sense on the value and challenges of cybersecurity for the organisation. Accordingly, we considered both strategic roles (directors, management) as well as tactical or operational roles (architects, consultants) as relevant for our interviews.

In doing so, we were able to capture insights from eight organisations on how they deal with realising cybersecurity by design. Table 1 provides an overview of the type of organisations that were interviewed. One can see that for our set of eight organisations, four organisations can be categorised as manufacturers of (digitalised) products or goods, two organisations as mobile telecom service providers, and two organisations as service providers in the context of (cyber)security.

Table 1 also indicates the type of roles our industry experts fulfilled at their respective organisations. One can see that a wide spectrum of roles has been interviewed, ranging from those present at C-levels in organisations as well as those active for hands-on product development. Accordingly, this gives us a broader perspective on how cybersecurity is realised within different facets of the organisation.

Table 1: Descriptives on the interviews conducted.

Type of organisation	Frequency	Type of roles interviewed
Manufacturer of (digitalised) products or goods	4	Technical director, solution architect, security architect, security risk manager, chief information security officer, chief product officer, product manager, security officer
Mobile telecom service provider	2	
Cybersecurity service provider	2	

Each interview was conducted using a standardised interview protocol, available in the Appendix of this report. As mentioned, this interview protocol was based on the barriers, drivers, incentives and challenges identified in literature. The following themes or topics were obtained:

- **Economic value of cybersecurity** – Deals with the added value of cybersecurity for organisations and customers in an economic sense, and the degree to which organisations perceive it as 'easy' or 'difficult' to communicate the value of cybersecurity.
- **Market influence on cybersecurity** – Concerns the developments in the market at competitors and suppliers on the adoption of cybersecurity, which can either complicate or stimulate the adoption of cybersecure practices by design.
- **Understanding and use of cybersecurity** – Touches upon the understandability of how cybersecurity can be applied and what it constitutes in practice. It deals with customers and organisations being able to explain how cybersecurity can be realised.
- **Compliance to legislation and policies** – Addresses the role of policy making and legal obligations to work towards cybersecurity by design and to adhere to formal standards and principles
- **Legacy of previous solutions and systems** – Concerns the role of legacy decision-making for products, solutions and systems on their design, which may impact the degree to which cybersecurity by design can easily, or even realistically, be achieved.
- **Human resources and cybersecurity expertise** – Considers the role of having access to human resources and knowledge on cybersecurity as a possible barrier or incentive to work towards cybersecurity by design.
- **Leadership and strategic decision-making support for cybersecurity** – Addresses the role of leadership and strategic decision-making power in organisations which advocate the inclusion of cybersecurity by design, and having access to internal resources to actively make changes in this respect to the organisation
- **Organisational culture and structure** – Touches upon the culture and structure present at the organisation which either motivates or discourages embedding cybersecurity by design for new product development.

Each interview took place via Microsoft Teams and took one hour to complete. Each interview was started with a short round of introductions. Subsequently, the interview protocol was used to detail the organisation of the respondent and to invite respondents to 'rate' the maturity of their organisation in terms of cybersecurity. Next, we discussed the general trends on cybersecurity that are present for the domain in which the organisation operates. This was followed by an in-depth analysis of the barriers, drivers, incentives and / or challenges that the organisation faced in either providing or realising cybersecure products, systems or systems-of-systems. Each interview was concluded by clarifying the most important barriers or drivers to transition towards cybersecure business practices by design. Interviews were recorded and transcribed, for which any confidential information shared was anonymised. Per interview, at least two TNO researchers were involved.

2.3 Analysis and sensemaking of results

Per **Step 3**, using the transcriptions of each interview, we cross-compared what drivers, barriers, incentives and / or challenges were mentioned. Using thematic analysis, we examined the data obtained through the interviews to draw conclusions on what drivers,

barriers, incentives and / or challenges were mentioned most or were considered as the most crucial in working towards cybersecurity by design.
In addition, we also sought to hypothesise why certain barriers or drivers were indicated by industry experts, given their respective organisation. For example, some drivers may be more prevalent related to the customer segments that organisations target, whether for others the products and services may demand additional care and attention for cybersecure practices, motivating principles of cybersecurity by design. This helped to further detail the results obtained.

3 Results of study

In this section, we detail the outcomes of our study. Through the series of interviews conducted, we identified several drivers and barriers that were frequently mentioned when realising cybersecurity. These can be categorised in themes related to cybersecurity and the **value for customers**, cybersecurity and **managing product development life cycles** and cybersecurity and **embedding within the organisation.** In the following section, we detail each of these themes.

3.1 Value for customers

All industry experts stressed the challenge of communicating the value of cybersecurity to their customers (or users). Despite the incidents we have seen over the past decades in terms of poor cybersecurity in products and services, with severe negative impact as a result, many customers still consider cybersecurity as a cost factor, rather than something that offers or creates value. This is largely due to the fact that cybersecurity aims to prevent threats from occurring, but these threats do not necessarily *have to* occur. Accordingly, embedding features for cybersecurity may not directly (or not even at all) lead to value. In response, customers may prioritise other aspects (performance, efficiency, robustness, safety) in favour of cybersecurity.

Several sub barriers can be associated to this theme:

Customers operating in low-margin markets may more quickly dismiss the desire for security updates or purchase more cybersecure, but expensive products. If customers need to keep the costs of products low to remain competitive in their respective markets, customers need to prioritise how this cost structure is shaped. As a consequence, customers will rather focus on product features which do not jeopardise the performance of the product, create immediate value, and can keep the cost price as low as possible.

Customers work with products that are 'core' to their operations, and hence availability **and time-to-market are more important to consider.** Some customers may also rely heavily on the products offered by manufacturers for their day-to-day operations, with downtime or outages having severe business impact for their bottom line. As the application of cybersecurity takes time (and can potentially lead to bugs or issues elsewhere), customers may be reluctant to adopt cybersecurity if it cannot be guaranteed that these issues can be avoided.

Customers do not always understand why additional cybersecurity features are needed or cannot adequately assess why the additional costs that enable (proper) cybersecurity are justified. We recognise from the interviews that customers struggle to understand why new cybersecure features are needed, and that it is often unclear what alternatives can be considered. It can occur that customers do not necessarily have expertise on what cybersecure solutions are possible or how standards in terms of security can be achieved through add-on services or updates. As a result, it becomes difficult for customers to justify the costs of cybersecurity.

Customers have different risk profiles, operate in markets or customers with different risks, and do not always conduct risk assessments. Moreover, customers can vary widely in their risk management approaches. Some customers are happy to accept a higher risk using outdated cybersecurity solutions or may perceive the impact probability of threats occurring to be low. The latter can occur for products which operate in relatively closed or small digital ecosystems. Accordingly, outsider threats are scarce and will only affect a limited set of connected products and systems, which may lead customers to 'accept' the risk (and hence not pursue cybersecurity) as the potential negative impact can be managed or mitigated.

Furthermore, some drivers have been identified:

Legislation such as NIS2 or CRA incentivise customers to look at whether products purchased comply with these standards, and also whether these products over time remain compliant. In many interviews, we see legislation acting as a driver for customers to uptake solutions that comply to current and upcoming legislation, as this gives these customers a right-to-play and access to market. If customers use products which are non-compliant, this may ultimately harm their profitability. Therefore, manufacturers of new products and services that are able to explicate that their products comply to cybersecurity or can help the customer in making products compliant through continuous updates, can as such 'sell' cybersecurity as a value proposition (giving the customer a 'right-to-play' if they select a manufacturer that is compliant). This can become an even greater selling point in case manufacturers can explicate that their products can sustain compliance over a greater period of time, as this means that customers can continue their products or services (i.e., limited downtime is expected), whereas customers also likely do not have to make subsequent investments into enabling cybersecurity.

In some cases, cybersecurity can be a differentiator, as products have reached high levels of maturity in other aspects. We have seen some cases for which cybersecurity became a selling point as it differentiated their products from the products offered by competitors. The advantages of added cybersecurity solutions can benefit the customer in various ways. For example, the regular updates and care for cybersecurity can lead to a mature product that is resilient against possible threats and attacks, resulting in decreased downtime. This value proposition can offset such products from those offered by competitors, particularly if such products are difficult to innovate on other aspects.

3.2 Managing product development life cycles

In our interviews, we observed different approaches towards integrating cybersecurity as part of product development, as well as dealing with product improvement across the product life cycle. One pertinent issue noted by almost all industry experts is the fact that cybersecurity evolves over time, hence keeping products cybersecure over time is challenging. This is due to the fact that products cannot always account for future cybersecurity developments, as such developments would have either made the product or service overly expensive (to account for threats which may not pose risks in the near future), or could not have been predicted yet (to account for threats which were unknown at the time of product development). Therefore, realising cybersecurity across the product life cycle, particularly when no set life cycle is given to products, is hard. However, such services have to be offered to protect the integrity and security of customer data (and sometimes has to be done to keep products compliant to ongoing legislation), but also to protect the trustworthiness and image of the organisations themselves. As a consequence, organisations need to decide between offering add-on

services, including cybersecurity maintenance as a long-term service, or refraining from updates over time.

Several sub-barriers can be associated to this theme:

Difficulty of dealing with changing requirements throughout life cycle. Although we observe that legislation can act as a driver for cybersecurity by design, as it increasingly incentivises customers to look for compliant products and services, these legislations and policies are also subject to change over time. Although organisations respond to this by establishing awareness on (and participation in) policy development, organisations cannot account for all future developments. Updates required to products to remain compliant require new investments, which either need to be contractually agreed upon with the customer, or need to be absorbed by the organisations themselves as a form of service provisioning. Depending on how frequently such updates would be needed, this can significantly complicate managing cybersecurity throughout the product life cycle.

Complex products that include components from different suppliers create further challenges in maintaining cybersecurity over the product life cycle. In addition to the above, for complex products, often components, products and services from suppliers and partners are integrated. Such offerings may also introduce additional digital features and hence need to be interconnected, meaning that cybersecurity does not depend solely on the focal organisation, but also depends on its suppliers and partners. When updating new products towards mature levels of cybersecurity, this means that suppliers and partners also need to update their components across the product life cycle. However, depending on how the collaboration between the focal organisation and suppliers / partners is set up, this is not necessarily a given: it may imply (re)negotiation with suppliers and partners to account for potential costs associated with updating cybersecurity. It also means that suppliers and partners need to align on how cybersecure features are implemented (such that they match those made by other suppliers or the focal organisation).

Dealing with legacy means that cybersecurity often becomes a quick fix instead of a long-term solution. Logically, products, services, and systems become outdated over time, but it would be inefficient to renew such products every time new versions are released. Moreso, products and services are sometimes used in core processes or centralised locations at customers making them difficult to remove or even to temporarily take offline as this will introduce downtime. Accordingly, as such products age over time, they will contribute more and more towards creating a legacy and outdated infrastructure, which will make them increasingly difficult to (keep) cybersecure. As a result of this, organisations are forced to make a decision between doing large cybersecurity overhauls (which will introduce significant costs and downtime for the customer) versus applying quick fixes (such as updating minor components or establishing increased cybersecurity in interfacing products and services). As organisations want to create immediate value for customers, quick fixes are often selected, but this also means that over time, maintaining cybersecurity will become an increasingly bigger challenge.

However, also an enabler was identified:

Having a clear understanding of what cybersecurity risks need to be incorporated at all times (and hence should be tackled 'by design') **can support setting up testing frameworks to guide product development.** Some cybersecurity risks hinge on design decisions made for the product which, when the product is released and operational, are difficult or even impossible to adjust without serious investments (since for example, they pertain to how the

product was designed or what core components were used). Accordingly, when developing new products and managing cybersecurity through the product life cycle, it is important that such risks can be assessed and are mitigated as much as possible to avoid any negative impact through the product life cycle. Accordingly, understanding these critical risks is important: it can help to set up testing frameworks for product development, to enable product development teams to test and evaluate whether their product can 'by design' account for or mitigate risks associated to key design decisions made. This enables organizations to avoid needing to rely on 'quick fix' cybersecurity solutions later on in the product life cycle, which may not be effective as they do not address the underlying design decisions made, or enable organizations to avoid costly efforts to rework the design of the product (possibly leading to potential downtime for the client).

3.3 Embedding cybersecurity within the organisation

In almost all interviews, embedding cybersecurity as part of the organisation was considered an important task, but also a significant challenge. Organisations recognise that in order to support cybersecurity by design in a systematic way, the importance of cybersecurity has to resonate on many layers of the organisations (not just on strategic levels, but also on operational levels) and has to be actively supported: without such support, cybersecurity is quickly referred to 'as another cost driver' which then often can be considered as strategically less relevant or less valuable as opposed to other cost drivers. However, realising this systematic change for the organisation is not trivial, and requires buy-in from strategic management as well as from employees working on product development. This change management that needs to take place takes time and requires ample resources and commitment to be successful.

The following sub-barriers were associated to this theme:

Creating buy-in at strategic management levels to consider cybersecurity as a key priority is difficult to achieve. Evidently, no organisation would consider the realisation of cybersecurity as 'unimportant', but organisations clearly have different priorities when it comes to cybersecurity versus other functional and non-functional product aspects. Although we frequently observe in our interviews that organisations adopt dedicated strategic roles for cybersecurity (like CISOs or CPSOs), which helps to create awareness on the need for and long-term development of cybersecure products, it does not necessarily mean that strategic decision-making will be geared towards cybersecurity – trade-offs still have to be made on all product aspects, and often such decisions are led by an economic focus. If the economic value of realising cybersecurity for new and existing products is difficult to communicate, this can still result in cybersecurity not being adopted by design.

Cybersecurity is sometimes considered as a 'burden' for development teams, imposed by **principles and standards for the organisation.** Some industry experts indicate that although cybersecurity principles and standards for the organisations are in place, with frameworks or models that employees can refer to, this does not necessarily lead to adoption of these principles by project development teams. This is largely attributed to the fact that efforts to make products more cybersecure can make the eventual products more costly or increase the time needed by project development teams to work towards prototype or marketable solutions. As development teams have to comply to strategic targets (quality, time-to-market, performance), additional requirements in terms of cybersecurity are as a result seen

as a burden. Moreover, principles and standards are not always a one-size-fits-all: some products require different cybersecurity approaches or call for a different implementation strategy. Understanding how this should be approached takes time, effort, and will as such also affect performance targets (meaning development teams might refrain from doing so) unless this is supported by the organisation.

Difficult for organisations to integrate cybersecurity as part of the organisation and to avoid thinking in silos. Experts also indicate that, although security business units are often present within the organisational structure, breaking the silos between business units is still a challenge. Each of the business units within organisations have different tasks, objectives and cultures. Often, communication and interaction between units occurs on a 'known' basis between employees or through formalised channels. As a result, even if the organisation dedicates resources and support towards enabling a business unit for cybersecurity, it is still difficult for the knowledge present at such units to proliferate effectively to other units (such as sales or product development). Accordingly, such units will often act upon their individual targets first before other considerations are taken into account.

4 Best practices and take-aways

Based on our results, categorised in terms of themes related to the customer, product and organisational structure, we propose a set of best practices and take-aways that emerged from the interviews. These are the following (as well as summarised in Figure 2):

1. **Rework cybersecurity from a product that can merely** prevent 'losing' value towards selling cybersecurity as a solution that can 'add' value

As illustrated, communicating the value of cybersecurity to customers was considered as one of the biggest challenges, customers have to choose between different cost drivers with cybersecurity not necessarily demonstrating immediate value (but rather to prevent losses in cases of threat occurrences). To deal with this, some solutions popped up through our interviews:

- Rather than offering cybersecurity as an add-on service (which in turn calls for subsequent iterations of decision making at the customer to realise cybersecurity in practice), cybersecurity can be incorporated as **part of the entire value proposition by design**. For example, through *as-a-service like propositions*, in which a product is offered as a service and hence continuously updated over time, cybersecurity updates can be compensated through the periodical fees paid by the customer. The customer as such receives the guarantee that the product achieves a certain performance level (availability, quality), independent from whether this stems from physical or virtual update and maintenance activities.

- An alternative to this can be to **cater cybersecure propositions to the risk profiles at customers**. As customers may have different risk appetites, customers may value (updates to) cybersecurity differently. Rather than taking a one-size-fits-all approach, which may imply that the organisation caters to the lowest needs for cybersecurity, products with different cybersecurity services can potentially be offered. As a result, the organisation can still develop and improve upon its cybersecurity expertise but can also cater to those customers that do not necessarily value cybersecurity by default.

- Another way to approach selling cybersecurity is to **connect cybersecurity to other functional and non-functional features** of the product that create value. For example, when working with robotics, safety of employees is considered as a key priority, and thus features heavily in product purchase and manufacturing. Such safety however can significantly depend on whether the product is mature in terms of its cybersecurity (i.e., to prevent outside attackers from accessing digital systems). Therefore, understanding how cybersecurity can create value for different product areas can help to justify the need for proper cybersecurity.

2. **Enabling cybersecurity-by-design calls for both top-down commitment as well as bottom-up adoption for the organisation**

Enabling cybersecurity requires all facets of the organisation to recognise the value of embedding cybersecurity-by-design and to possess the resources (capabilities, knowledge, incentives, finances) to do so. The following best practices were indicated for our set of interviews:

- To support the bottom-up adoption for the organisation, industry experts advocate establishing **multi-layered training programs** to create awareness, educate and train employees proactively in terms of cybersecurity by design. Such a training program would constitute:
    - Basic yet obligatory courses on dealing with cybersecurity for *all* employees, such that awareness on the importance of cybersecurity (and basic principles to deal with cybersecurity by design) can be instilled.
    - Intermediate yet optional courses for employees interested to learn more about how cybersecurity by design can be enabled, providing more detailed insights and training to employees to include cybersecurity as part of their day-to-day operations.
    - Advanced, generally long-term courses for employees interested in becoming a 'security champion', i.e., employees that act as a spokesperson or representative to other employees on how cybersecurity by design can be tackled. Such employees enact this role as security champion in addition to their actual position at the organisation and can, on the operational level, offer quick(er) input to other employees on dealing with cybersecurity challenges.

For the latter two training programs, sufficient resources should be made available to encourage and incentivise employees to educate themselves on how cybersecurity by design can best be enabled. This is to prevent such training programs to be considered as 'another task', which may conflict with the performance objectives as part of their current position in the organisation (and hence employees may refrain from taking such courses).

- Another solution identified was to provide operational support on dealing with cybersecurity challenges at various levels for the organisation, such that the gap between the strategic level (at which cybersecure principles are defined and enacted) and the operational level (at which the principles are integrated for product development) can be bridged. Examples include the inclusion of organisational structures such as **cybersecurity boards** (which offer a more direct line to management on how principles have been defined), **cybersecurity support units** (offering direct support and guidance to employees on how cybersecure principles can be integrated), **cybersecurity communities** (in which employees can offer hand-on feedback to others on how challenges faced for cybersecurity can be resolved, as well as to offer best practices learned).

- A final solution that was mentioned is the formal inclusion of **security architects** for development teams to ensure when product development and improvement takes place, the level and maturity of cybersecurity is continuously assessed, and necessary adjustments can be made. The role of the architect is to ensure that products adhere explicitly to the principles and standards set at the strategic level (and is knowledgeable on what these principles and standards are), and actively works together with the engineers to realise this. Accordingly, the security architect acts as a liaison between the development teams and strategy.

3. To work towards cybersecurity by design, organisations need to transition from fixed life cycles towards continuous, yet flexible product life cycles

To be cybersecure by design over a long period of time means that products need to be continuously updated and renewed over time, in order to account for changing threats and trends occurring within the digital ecosystem. This means that organisations should not treat products with a finite lifetime (which may lead organisations to adopt a short-term perspective on how cybersecurity should be managed), but rather look at how updates to cybersecurity can be considered over an 'infinite' lifetime. The following best practices were given:

- To work towards continuous product cycles, industry experts indicate that organisations should work towards products which are **modular** in terms of managing cybersecurity. Ideally, parts of the products can periodically be updated without (severely) jeopardising the operation and performance of the product (i.e., meaning the customer may face downtime), as these parts can relatively independently be worked on. This may imply that other functions of the product can still be used, or the product as a whole can (potentially at a lower intensity) still be operated.

- In addition, to deal with the challenge of balancing the risk of not having cybersecurity versus the cost of realising cybersecurity (justifying whether cybersecure updates to new products should be made), organisations should incorporate **flexibility** as part of their risk assessment approaches (and avoid a binary yes or no decision): when doing risk assessment, organisations can also assess whether updates for cybersecurity can potentially be trimmed down (to cut down on costs) or whether risks can be mitigated (to ensure availability of the product), as long as it is clear how such partial measures will impact the next update cycle and how cybersecurity in the long run can still be safeguarded. This may imply that several small updates can be considered before a large update is needed. It can also mean that products which are not necessarily cybersecure by default (for example using old legacy systems) can be made cybersecure by ensuring that the systems with which it interacts are made *more* cybersecure.

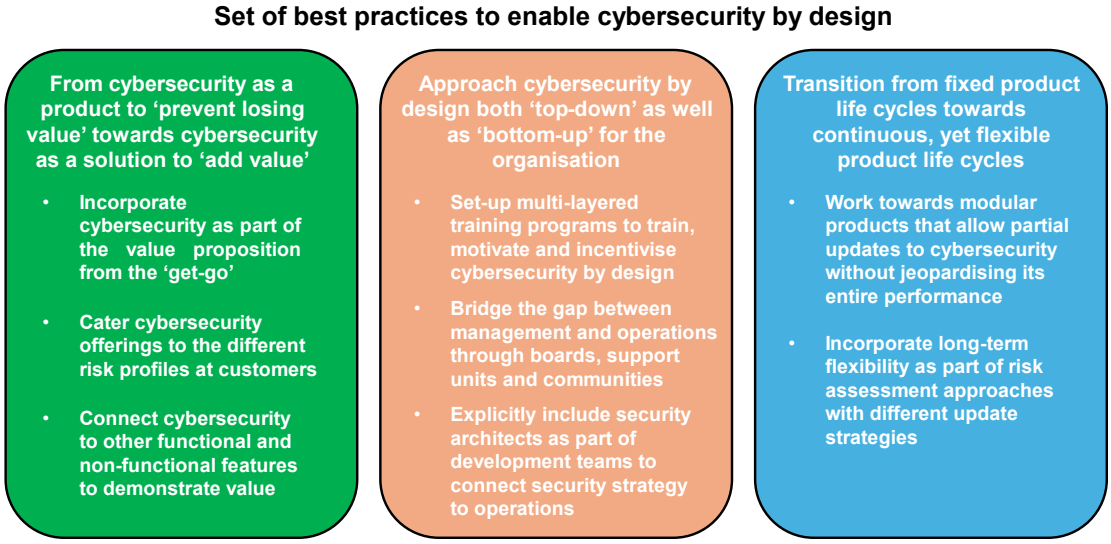

Figure 2: Summary of best practices to enable cybersecurity by design identified.

5 Outlook and next steps

The work presented in this report may help organisations, specifically manufacturers that are working towards cyber-physical products and systems, to take steps towards realising cybersecurity by design as part of their product development and improvement processes. The best practices identified can serve as the basis for reflection as well as innovation for organisations wishing to do so.

Our findings are based on an initial set of interviews: accordingly, the results are preliminary, and we intend to update these results over time as additional interviews with organisations are held. In this light, the objective is to validate the current set of best practices as well as include additional opportunities to consider. To do so, we intend to include interviews with organisations active in the banking industry: given the market they operate in, the type of products and services they offer (which are highly digitalised), and the type of information and transactions they need to manage, such organisations may offer additional insights on how cybersecurity by design can be realised in practice.

In addition, our intention is to complement our current findings, which are qualitative in nature, with evidence from case studies in which organisations are moving towards cybersecurity by design. Specifically, we intend to investigate how the best practices listed can best be applied to organisations, to evaluate the costs associated to such changes, and to assess in broad terms what the impact can be on the level of compliance to contemporary cybersecure standards and principles for new and developed products.

Lastly, we are exploring how the findings and best practices can be integrated as part of current product development methodologies: accordingly, guidelines and recommendations can offered on how organisations can seamlessly integrate cybersecurity as part of their development approaches.

Appendix

Interview protocol used to guide the semi-structured interviews

General description

- Can you describe your organisation and your position in more detail?
- What experience do you have with cybersecurity?

Cybersecurity in general

- What role does cybersecurity play for your organisation?
- Would you consider cybersecurity at your organisation to be 'strong'? why?
- What is the impact of having access to cybersecure solutions for your organisation?
- Are there examples of cases in which you felt cybersecurity to be insufficient for your organisation?
- How do you see developments within your domain regarding cybersecurity?
- What are the current trends on cybersecurity, in terms of market and regulation?

Barriers and incentives

- What barriers do you see in terms of implementing cybersecurity by design?
    - **Economic** – can the value of cybersecurity be explained to customers? Do customers perceive cybersecurity as economically important?
    - **Market** – what is the influence of the market on cybersecurity (threats, suppliers)?
    - **Understanding and use** – Is it understandable how cybersecurity can be used? Is it clear how technologies and solutions contribute to cybersecurity? Is it easy to use cybersecure solutions?
    - **Compliance** – Does legislation help to encourage, or make it difficult to adopt cybersecure practices? Is certification rewarded?
    - **Legacy** – is it difficult to implement cybersecurity as current systems are not necessarily compatible?
    - **Human resources** – is there expertise available in-house to support cybersecure practices, or to develop solutions in-house? Do employees understand why cybersecurity is necessary, and how it can be applied?
    - **Leadership** – is cybersecurity supported through leadership? Are structures, systems in place that support the strategic relevance of cybersecurity within the organisation? Are resources available to support cybersecurity development and to create initiatives to stimulate cybersecurity?
    - **Organisational culture and support** – is there training available to support cybersecure practices? are norms and values for proper cybersecurity encouraged by the company?

Future directions

- What is your future outlook on how cybersecurity for your organisation will develop?
- What is in your opinion crucial to work towards cybersecurity by design on a long-term basis?
- What current developments do you see as promising in enabling the transition to cybersecurity by design?
- What resources would you need to realise cybersecurity by design in the future?