Computer Law & Security Review 52 (2024) 105914

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models

Christof Koolen [a,*], Kim Wuyts [b], Wouter Joosen [b], Peggy Valcke [a]

[a] Centre for IT & IP Law, KU Leuven, Belgium
[b] Department of Computer Science, KU Leuven, Belgium

ARTICLE INFO

Keywords:
Cybersecurity
Appropriate technical and organisational measures
IT systems
GDPR
Risk assessment
Compliance obligations

ABSTRACT

Cybersecurity is a much-debated topic in both technical and legal scholarship. With contemporary business models hinging on highly performant information systems, there is increased awareness among entrepreneurs that security incidents often have devastating consequences on undertakings' revenue streams, intellectual property, and brand reputation. As a result, there is an increased focus on the obligation to implement cybersecurity measures. In the context of the GDPR, cybersecurity obligations seem to converge on the requirement to deploy 'appropriate technical and organisational measures' in order to ensure a level of security commensurate with the risks posed to an organisation. Yet, given the complex and rapidly evolving nature of the subject matter, the precise meaning and scope of these obligations remain unclear. This contribution offers guidance on how to assess the concept of 'appropriate technical and organisational measures' by considering it through the lens of cybersecurity maturity models. Accordingly, this article provides anchorage to scholarly audiences when scrutinizing the extent to which privacy and security measures qualify as 'appropriate' in the context of liability claims and actions for damages, thereby creating an opportunity to move from technical insight to legal compliance.

1. Introduction

Digital technology permeates practically every aspect of present-day commerce. Ranging from sensory driven business models to personalised shopping experiences, it appears that the enterprise of tomorrow is built on information and communication technology (ICT) where the seamless integration between platforms, software, and hardware is key. In the same vein, market studies indicate that SMEs attach great importance to business digitisation as it facilitates the acquisition of new customers and is conducive to brand expansion.[1] From a purely entrepreneurial point of view, digitisation is thus associated with productivity increases and costs reductions, thereby putting firms in a position to gain a competitive edge over their non-digitised counterparts.

The benefits of digital innovation for consumer markets should not be neglected either. With internet connectivity being readily available in family households, a strong uptick of high technology products such as smart devices[2] and subscription-based software[3] is noticeable. Whether it is a desire to remain connected with peers or a wish to gain detailed insights into one's own lifestyle, digitisation also offers interesting value propositions to many end users.

Notwithstanding the positive effects of digitisation on everyday life, an extensive reliance on technology-infused infrastructure also implies

* Corresponding author at: KU Leuven, Faculty of Law, Tiensestraat 41, 3000, Leuven, Belgium
E-mail address: christof.koolen@kuleuven.be (C. Koolen).

[1] Statista Research Department, 'Business Digitization' (*Statista*, 21 January 2021) <https://www.statista.com/topics/3127/business-digitization/> accessed 19 May 2022.

[2] E.g., Rolf H Weber and Evelyne Studer, 'Cybersecurity in the Internet of Things: Legal Aspects' (2016) 32 Computer Law & Security Review 715, 715.

[3] E.g., Alexander Savelyev, 'Software-as-a-Service – Legal Nature: Shifting the Existing Paradigm of Copyright Law' (2014) 30 Computer Law & Security Review 560, 561.

https://doi.org/10.1016/j.clsr.2023.105914

Available online 16 November 2023

that occurrences of security threats[4] and incidents are likely to increase.[5] As technology continues to advance and more devices and systems become connected to the internet, the cybersecurity sector is confronted with a growing number of difficulties in ensuring protection against cyberthreats. It is especially the current level of sophistication of IT systems[6] that brings various security challenges with it, for example protection against DDoS attacks[7], malware[8], data breaches and zero-day exploits[9]. Such problems—and especially their consequences—are often magnified when enterprises integrate vulnerable software or devices into their existing networks.

Several recent, high-profile security incidents confirm that adequate cybersecurity is crucial.[10] Awareness surrounding this topic has created an impulse for the European legislator to thoroughly review the legal landscape apropos cybersecurity in the late 2010s and to update existing views on IT security.[11] At present, the applicable rules on EU cybersecurity law lie dispersed across several legal instruments[12]; dispersion which may give rise to demarcation issues and interpretative difficulties for stakeholders. These challenges notwithstanding, the focal point of the GDPR lies on the requirement to adopt '*appropriate technical and organisational measures*' to ensure '*a level of security appropriate to the risk*'.[13]

Although convergence[14] towards the concept of appropriate technical and organisational measures is noticeable, it is difficult to arrive at a profound understanding of its meaning. Moreover, some uncertainty surrounds the relationship between the requirement to implement appropriate security measures and the requirement to ensure an appropriate level of security relative to the risks. The goal of this contribution is to offer guidance on this topic by combining legal and technical insights. More specifically, the emphasis is on *analysing the appropriateness of cybersecurity measures through the lens of cybersecurity maturity models*. Fundamentally, these cybersecurity maturity models are understood as methodologies that organisations can use to assess and improve their cybersecurity posture. As such, they are intended to serve as a structured guidepost with progressively more sophisticated objectives for implementing cybersecurity practices.

At present, cybersecurity is no longer a niche subject matter and, thus, calls for a rapprochement between legal and technical scholars[15] should be acknowledged. By seeking common ground between law and technology and by relying on an interdisciplinary approach, the aspiration is to enable IT professionals to get a better grasp of the applicable legal tests while providing lawyers with a deeper understanding of what is technically feasible in terms of cybersecurity measures. The combination of both views should enable stakeholders to move from isolated insights to joint legal compliance.

The following structure is used to attain this objective. Section 1 first sheds light on the conceptualisation of cybersecurity requirements. Section 2 subsequently scrutinises the notion of 'appropriate technical and organisational measures' under the GDPR. Dedicated subsections discuss the appropriateness of technical measures (2.1), organisational measures (2.2), and the proportionality dimension (2.3) respectively. After that, Section 3 combines the legal and technical insights in view of offering further clarifications as to the implications of (in)appropriate cybersecurity measures.

2. Conceptualisation of cybersecurity requirements

Cybersecurity rules do not lend themselves well to be set in stone. One of the main challenges faced by policymakers is that cybersecurity is a moving target: what is considered secure today may well be insecure tomorrow.[16] The rapid rate of industry change and evolving understanding of cybersecurity bring about a climate where it is quite

[4] Consider Donald Firesmith, 'Specifying Reusable Security Requirements.' (2004) 3 Journal of Object Technology 61, 63 who defines a security threat as: "*a general condition, situation, or state (typically corresponding to the motivation of potential attackers) that may result in one or more related attacks*".

[5] Duance C Wilson, *Cybersecurity* (MIT Press 2021) 4.

[6] The term 'IT systems' is to be interpreted in a broad sense, referring to all types of IT-based assets, including products, services, and infrastructure.

[7] Distributed Denial of Service (DDoS) attacks involve flooding IT systems with connection requests in an attempt to overload the system and render it inaccessible. The attack is 'distributed', which means that it originates from several different sources, thus rendering it impossible to stop the attack by only blocking one perpetrator's access. For an in-dept discussion of this topic, see Jennifer A Chandler, 'Security in Cyberspace: Combatting Distributed Denial of Service Attacks' (2004) 1 University of Ottawa Law & Technology Journal 231, 236 ff.

[8] Malware encompasses a file or piece of code that is maliciously put on IT infrastructure, where it wreaks havoc by disrupting core functionality, leaking data or, more generally, interfering with the overall user experience. By way of illustration, file-encrypting ransomware saw a significant surge in 2021 following the increasing popularity of cryptocurrency. In this respect, see Masarah Paquet-Clouston, Bernhard Haslhofer and Benoît Dupont, 'Ransomware Payments in the Bitcoin Ecosystem' (2019) 5 Journal of Cybersecurity 1, 2.

[9] A zero-day exploit revolves around a vulnerability in software that is unknown to its programmer. The aspect 'zero-day' specifically refers to the number of days since the release of the software package. Accordingly, it implies that the vulnerability was contained within the software at the time of its release.

[10] Notable examples include the 2017 WannaCry ransomware attack and the 2016 Mirai botnet DDoS attacks; for an authoritative source to highlight the growing relevance of cybersecurity threats, see Claudio Ardagna and others, 'ENISA Threat Landscape 2022' (2022) ENISA Report <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022> accessed 13 April 2023.

[11] Recent developments in this respect include the entry into force of the NIS2 Directive on 16 January 2023, thereby repealing the 2016 Network and Information Security Directive: Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union [2022] OJ L 333/80 (hereafter: NIS2 Directive).

[12] ibid; Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification [2019] OJ L 151/15 (hereafter: Cybersecurity Act); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (hereafter: GDPR); Alessandro Mantelero and others, 'The Common EU Approach to Personal Data and Cybersecurity Regulation' (2021) 28 International Journal of Law and Information Technology 297, 327: several sector-specific instruments, such as the revised Payment Service Directive (hereafter: PSD2) for payment instruments and the eIDAS Regulation for electronic identification, also exist.

[13] Article 32, GDPR.

[14] Consider, for instance, the following provisions. Article 21, NIS2 Directive: "*Member States shall ensure that essential and important entities take* appropriate and proportionate technical, operational and organisational measures to manage the risks *posed to the security of network and information systems*"; Article 95, PSD2: "*Member States shall ensure that payment service providers establish a framework with* appropriate mitigation measures and control mechanisms to manage the operational and security risks*, relating to the payment services they provide*"; Article 19, eIDAS: "*Qualified and non-qualified trust service providers shall take* appropriate technical and organisational measures to manage the risks *posed to the security of the trust services they provide*".

[15] Including our own in an earlier edition of this journal; see Peggy Valcke, Inge Graef and Damian Clifford, 'IFairness – Constructing Fairness in IT (and Other Areas of) Law through Intra- and Interdisciplinarity' (2018) 34 Computer Law & Security Review 707.

[16] As eloquently put by Iain Nash, 'Cybersecurity in a Post-Data Environment: Considerations on the Regulation of Code and the Role of Producer and Consumer Liability in Smart Devices' (2021) 40 Computer Law & Security Review 1, 2: "*[t]he relevance and importance of cybersecurity in legal theory should be evaluated within the context of the changing nature of computing*".

challenging to adopt legal norms. Overly specific rules risk being outdated before the ink has even dried. Oppositely, vaguely worded provisions are difficult to transpose into practice.

Thus far, the EU legislator's approach coincides with using a broadly worded and technology neutral[17] standard of care, therefore leaving matters of detail open to interpretation.[18] While understandably frustrating from an industry perspective, it is difficult to fault policymakers for pursuing this route when considering some of the underlying reasons as to why cybersecurity is such a complex subject matter. For instance, the multitude of potential attack vectors[19] and the fact that IT systems are embedded in complex digital ecosystems[20] are just two factors that come to mind.

As a result, the introduction of new legal rules concerning the security of IT systems is a time-consuming and tedious process that is very much prone to error. Because technology is in a constant flux, it is not easy to quickly respond to new developments from a legislative point of view. This explains why hard law approaches are often supplemented by soft law instruments, such as standards[21] and industry guidelines.[22] However, while these documents are certainly useful, they are rather ineffective in providing a high level of legal certainty for tech entrepreneurs looking to protect their interests (i.e., reputation, intellectual property, customer relations) and delineate their legal liability. As a result, it can only be concluded that there is no universal legal approach towards cybersecurity.[23]

Despite these challenges, the overarching objective of cybersecurity instruments is clear: to effectively protect IT systems and to have a deterrent effect on cybercriminals. To that end, the GDPR explicitly makes mention of a cybersecurity benchmark. More specifically, it mandates that *appropriate technical and organisational measures* (ATOM) should be put in place in order to ensure *a level of security appropriate to the risk*. [24] As argued by Hofman, a clear means-end relationship exists between these two elements: the appropriateness of the adopted security measures (i.e., the means) serves as a prerequisite for achieving an appropriate level of security (i.e., the end result).[25] In other words, the security measures taken play an instrumental role in achieving an appropriate security level.[26]

At this point, following a close reading of the GDPR, it is shown that the legal standard used to assess cybersecurity revolves around the ATOM benchmark. This benchmark emphasises that security measures should be attentive to the impact of any security risks that might occur, whilst having regard to the state of the art. In other words, cybersecurity measures must provide a level of security that is commensurate with the risks that might occur.[27] This subsequently leads to the following closed-loop reasoning. On the one hand, to determine the appropriateness of security measures, the appropriate level of security must first be identified in light of the potential security risks. On the other hand, to attain an appropriate level of security, appropriate security measures must be adopted. Ultimately, this boils down to a clear risk-based approach in the GDPR; a line of thinking that will be further explored below.[28] That being said, organisations enjoy a high degree of freedom to take the security measures they deem appropriate for their IT systems. This freedom is rooted in two elements. Firstly, the fact that the organisation itself is best positioned to determine the level of risk associated with its goods and services, which then leads to the determination of an appropriate level of security, which then requires the adoption of ATOM. Secondly, the fact that security issues can be addressed in a variety of ways. Thus, it depends on the organisation, the underlying context, etc. to determine which solution is most appropriate given the specific circumstances.

Absent further clarifications, however, the discussion quickly veers towards the exact meaning and mode of application of the ATOM benchmark and how it relates to the requirement to ensure an appropriate security level. In this context, it can only be concluded that the noticeably imprecise nature of the ATOM benchmark acts as a double-edged sword. Admittedly, its general wording ensures that the benchmark will stand the test of time.[29] Concurrently, as argued elsewhere by Weber, the norm itself is rather nebulous and does not truly provide clear answers to entrepreneurs how they should secure their IT systems.[30] Apropos the specific measures to be taken, some inspiration can be drawn from the GDPR, which lists measures such as encryption, pseudonymisation, integrity checks, back-ups, and security testing procedures.[31] For the purposes of assessing the significance of a cybersecurity incident, the NIS2 Directive also suggests looking at factors such as the number of affected users, the duration of the incident, and whether the organisation adhered to approved codes of conduct.[32] Some further guidance can also be found in several reference documents, notably those stemming from ENISA[33] and national Data Protection Authorities.[34] Notwithstanding the persuasive value of these documents, they rarely contain clear-cut instructions for real-world use cases and sometimes fall short in terms of their action-oriented nature. Moreover, it must also be acknowledged that an element of timeliness may affect the validity of any reference documentation that is not regularly revised and kept up to date.

Considering the foregoing and in the face of limited further explanation, it is therefore necessary to interpret[35] the ATOM standard and scrutinise more closely how it would be applied. In line with other legal writings, it follows that the standard consists of two separate elements that are supplemented with a balancing test:[36]

[17] Cf Recital 15, GDPR.

[18] David Bomhard and Andreas Daum, 'Cybersecurity in Outsourcing and Cloud Computing: A Growing Challenge for Contract Drafting' (2021) 2 International Cybersecurity Law Review 161, 167; Weber and Studer (n 2) 726.

[19] Erick Buenrostro and others, 'Security of IoT Devices' (2018) 2 Journal of Cyber Security Technology 1, 7; Weber and Studer (n 2) 719; Michael J Covington and Rush Carskadden, 'Threat Implications of the Internet of Things', *5th International Conference on Cyber Conflict* (2013) 12.

[20] Pier Giorgio Chiara, 'The IoT and the New EU Cybersecurity Regulatory Landscape' (2022) 36 International Review of Law, Computers & Technology 1, 12.

[21] E.g., ISO, 'Information Security Management Systems' (2018) ISO/IEC 27000:2018.

[22] E.g., National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure Cybersecurity' (National Institute of Standards and Technology 2018) NIST CSWP 04162018 <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> accessed 17 January 2023.

[23] Worku Gedefa Urgessa, 'Multilateral Cybersecurity Governance: Divergent Conceptualizations and Its Origin' (2020) 36 Computer Law & Security Review 1, 2; Weber and Studer (n 2) 716–717.

[24] Article 32, GDPR.

[25] Janita Hofman, *De beveiliging van persoonsgegevens: Over de juridische invulling van art. 5 lid 1 onder f en 32 AVG* (Wolters Kluwer 2022) 49–52.

[26] ibid 50.

[27] Mantelero and others (n 12) 327.

[28] See below at Section 2.3.

[29] Bomhard and Daum (n 18) 167.

[30] Weber and Studer (n 2) 726; see also Lachlan Urquhart and Derek McAuley, 'Avoiding the Internet of Insecure Industrial Things' (2018) 34 Computer Law & Security Review 450, 460.

[31] Article 32, GDPR.

[32] Article 32(7) NIS2 Directive.

[33] E.g., on the topic of pseudonymisation: ENISA, 'Deploying Pseudonymisation Techniques: The Case of Health Sector' (2022) 1 <https://data.europa.eu/doi/10.2824/092874> accessed 8 March 2023.

[34] E.g., on the topic of (securely) processing biometric data: Belgian Data Protection Authority, 'Aanbeveling Betreffende de Verwerking van Biometrische Gegevens' (2021) 33 <https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.01-2021-van-1-december-2021.pdf> accessed 8 March 2023.

[35] Weber and Studer (n 2) 726.

[36] Mantelero and others (n 12) 327–328; Urquhart and McAuley (n 30) 459–463.

(i) Appropriate technical measures
(ii) Appropriate organisational measures
(iii) Measures proportionate to the security risks and implementation costs

Compliance means that both types of measures—technical ones and organisational ones—should form an integral part of a firm's governance framework, thereby also underscoring that they encompass long-term obligations rather than a set-and-forget approach.

In search of more meaningful answers, it is sensible to bring cybersecurity practitioners to the forefront in order to supplement the legal approach taken towards cybersecurity with more tangible insights. In our view, this step is both useful and necessary to overcome the implementation gap that currently exists between how cybersecurity requirements are drafted from a legal point of view and how cybersecurity requirements are implemented from a practical standpoint. While some may not prefer to take this claim at face value, it must be emphasised that such approach also corresponds to legal practice, where court claims are either corroborated or debunked by virtue of expert evidence submitted by IT experts. Hence, by conjoining both legal and technical perspectives, concrete steps can be taken towards answering questions vis-à-vis the level of cybersecurity entrepreneurs should provide for their IT systems. In doing so, the remainder of this article provides anchorage to scholarly audiences and guideposts for practitioners when scrutinising the extent to which security measures qualify as 'appropriate', thereby creating an opportunity to move from technical insight to legal compliance.

3. Appropriate technical and organisational measures

It is worth noting that IT systems do not appear out of thin air. Metaphorically, a comparison can be drawn with constructing a house. Firstly, a soon-to-be homeowner presents their vision to an architect. Secondly, the architect translates these ideas into assorted blueprints and other structural drawings, which outline the building's specifications, floor plan, and materials to be used. Thirdly, the blueprints are subsequently relied on by a construction crew to commence work at the building site. While doing so, the constructions workers regularly liaise with the architect to ensure the correct implementation of the blueprints. Fourthly, once the construction project has been completed, a final inspection is conducted to ensure that no construction mistakes were made, that the building's utilities were properly set up, and that the homeowner's requirements were met. Fifth, the home is turned over to the homeowner, who sets up their furniture and belongings and moves in.

The creation of IT systems follows a similar, multi-stage process. Consider, for instance, the terminology of Izar Tarandach and Matthew Coles' five-phase development methodology:[37]

(i) *Idea inception*: conceive an idea for an IT system; work out the needs and wants of the relevant stakeholders.[38]
(ii) *Design*: define specific goals and translate stakeholders' requirements into an IT architecture.
(iii) *Implementation*: build the IT system based on the specifications of the design phase.
(iv) *Testing*: verify whether the implemented IT system continues to meet stakeholders' requirements
(v) *Deployment*: launch[39] of the IT system, application, or feature; proper maintenance of the IT system once it is deployed.

It is important to note that these phases are not to be seen as one-time sequential walk-throughs: output of activities from each of the phases is regularly fed back to previous phases, as IT system development is a continuous process.[40] In line with the above metaphor, once the home is occupied, regular maintenance will be required to prevent malfunctions.

Within this development lifecycle, security and privacy need to be embedded *by design*.[41] To return to the construction metaphor: when building a house, electricians and plumbers are brought in prior to the completion of the construction works. By involving these tradespeople early on, the wiring and plumbing can be embedded into the foundation of the house. This is referred to in the GDPR as 'appropriate technical measures'.[42] In addition to the inclusion of technical measures, firms must also lay out strategies, policies, and guidance for their overall development practices. This overarching *governance* angle to IT system engineering is equally focussed on ensuring security and privacy, and is referred to as 'appropriate organisational measures' in the GDPR.[43]

To determine whether a particular firm is on the right track, IT professionals seek recourse to *cybersecurity maturity models*.[44] These models provide a means to assess and strengthen the security posture of an organisation. Among others, a maturity model can be used to define a suitable cybersecurity implementation strategy and aid in laying out a roadmap with future steps that could further improve an organisation's security practices. Several maturity models and frameworks exist that can assist firms in fortifying their IT systems. Notable examples include:[45]

- OWASP's[46] Software Assurance Maturity Model (SAMM)[47].
- Building Security In Maturity Model (BSIMM)[48].

[37] Izar Tarandach and Matthew Coles, *Threat Modeling: A Practical Guide for Development Teams* (1st edn, O'Reilly Media 2021) xxiii; note that minor terminological differences exist among the relevant scholarly sources and that some authors introduce slight variations or subdivisions within this multi-stage process: Youssef Bassil, 'A Simulation Model for the Waterfall Software Development Life Cycle' (2012) 2 International Journal of Engineering 1, 2; OWASP, 'OWASP in SDLC' (*OWASP Foundation*, 5 May 2021) <https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdlc/> accessed 13 February 2023.

[38] Phase (i) falls outside the scope of the cybersecurity measures discussed in this paper.

[39] Note that, depending on the granularity of the development practice, 'launching a system' can either concern the launch of a full IT system or—in more agile development operations—smaller, individual system features.

[40] Tarandach and Coles (n 37) xxv: "It is important to emphasize that threat modeling is an evolutionary process. You may not find all the flaws in your system the first time it is analyzed".

[41] Recital 78, GDPR; Article 25, GDPR.

[42] See below at 2.1; Article 32, GDPR.

[43] See below at 2.2; Article 32, GDPR.

[44] Jay Payette and others, 'Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects' (2015) 5 Technology Innovation Management Review 26; Walter Miron and Kevin Muita, 'Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure' (2014) 4 Technology Innovation Management Review 33; Gregory B White, 'The Community Cyber Security Maturity Model', *2011 IEEE International Conference on Technologies for Homeland Security* (2011) 173.

[45] For a comparison between some of the different maturity models, consider Brian Glas, 'Comparing BSIMM & SAMM' (*OWASP SAMM*, 29 October 2020) <https://owaspsamm.org/blog/2020/10/29/comparing-bsimm-and-samm//> accessed 13 February 2023.

[46] The Open Web Application Security Project (OWASP) is a community of security researchers that creates and shares articles, documentation, and tools to advance the field of cybersecurity.

[47] OWASP, 'OWASP SAMM - Version 2' (2021) OWASP Foundation <https://drive.google.com/file/d/1cI3Qzfrly_X89z7StLWI5p_Jfqs0-OZv/view?usp=sharing&usp=embed_facebook> accessed 17 January 2023.

[48] X, 'Building Security In Maturity Model' (*BSIMM*, 1 September 2022) <https://www.bsimm.com/> accessed 17 January 2023; X, 'BSIMM13' (BSIMM 2022) Foundations Report 2022-Version 13 13 <https://www.bsimm.com/content/dam/bsimm/reports/bsimm13-foundations.pdf?cmp=pr-sig&utm_medium=referral> accessed 17 January 2023.

- NIST's[49] Cybersecurity Framework (CSF)[50], Secure Software Development Framework (SSDF)[51], and Privacy Framework.[52]

In the remainder of this section, the focal point lies on OWASP's SAMM to further expand on security practices that could—and should—be applied in each phase of the IT system development lifecycle. While each maturity model puts accents on specific areas, the alternative frameworks include comparable practices that would ultimately converge towards a consistent assessment of an organisation's security posture.

OWASP's SAMM starts from the presumption that there is no single cybersecurity recipe that works for all firms.[53] Instead, the model identifies an assorted series of security practices that apply to the different stages of the IT system development lifecycle. Subsequently, each of these practices is divided into three different tiers—commonly referred to as *maturity levels*. These maturity levels have progressively more sophisticated aims and more demanding success metrics, thus permitting firms of varying complexity to benchmark their security posture.[54] For each security practice, the three maturity levels can be conceptualized as follows:

- Level 1 – Ad-hoc approach
- Level 2 – Increased efficiency and effectiveness
- Level 3 – Comprehensive mastery at scale

Furthermore, the maturity levels are structured into two streams, each covering a different aspect of the security practice. For instance, to perform a proper threat assessment, one can focus on building a risk profile (i.e., classify systems on the basis of their risk) as well as engage in threat modelling (i.e., identify architectural design flaws).[55] The application of the SAMM to the threat assessment practice is illustrated below in Table 1.

Approaching cybersecurity through the lens of maturity levels has three distinct objectives.[56] Firstly, it offers *measurable insights* into security practices. Secondly, it provides *actionable pathways* for improving a firm's security posture. Thirdly, it remains *versatile* across different organisations, technologies, and processes.

From a more academic perspective, cybersecurity maturity models lend themselves well to permit organisations to identify the level of security they should adhere to within the maturity model. First and foremost, this requires a thoughtful process that takes several factors into account, including the organisation's size, the industry in which it operates, the data that it processes, the risks that it faces, and budgetary considerations. In a subsequent step, by facilitating the identification of the relevant maturity level, cybersecurity maturity models provide a roadmap for determining the technical and organisational measures that should be adopted to attain the envisioned maturity level. As such, cybersecurity maturity models fit well with the goal of recognising that cybersecurity involves a risk-based approach, where not all organisations are exposed to the same level of risk. By stressing the adoption of measures appropriate to the specific context (i.e., the means), maturity models force entities to think critically about the risks they face, and allow them to identify the corresponding level of sophistication of the measures required to mitigate those risks, thereby contributing to an appropriate level of security (i.e., the end result).

3.1. Appropriate technical measures

3.1.1. Technical maturity levels

The notion 'appropriate technical measures' refers to the safeguards that firms must implement and apply to their hardware, software, and networks in view of ensuring compliance with the CIA triad[57] and the privacy triad.[58] The term 'technical' is interpreted broadly and typically denotes practical ways and methods of pursuing security (e.g., encryption, access controls, intrusion detection systems, etc.).[59]

In the context of OWASP's SAMM, technical security measures are mapped to stages (ii)-(v) of the IT system development lifecycle (i.e. *design, implementation, verification*, and *operations*).

3.1.2. Design

During the design phase of IT systems, the requirements and specifications of the system are outlined, and the system's architecture is defined. OWASP's SAMM highlights three key security practices that need to be considered at that time: assessing threats, identifying security requirements, and designing a secure architecture.[60]

Threat assessment. It is broadly understood that it is much more cost-effective to introduce changes during the design phase of a system rather than making modifications when the system is already operational. Therefore, it is important to consider all potential security issues that could arise in the IT system in the future. In this context, *threat*

[49] The National Institute of Standards and Technology is a US-based organisation that strives to promote innovation.

[50] National Institute of Standards and Technology, 'Cybersecurity Framework' (*NIST*, 12 November 2013) <https://www.nist.gov/cyberframework> accessed 17 January 2023; National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure Cybersecurity' (n 22).

[51] Murugiah Souppaya, Karen Scarfone and Donna Dodson, 'Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities' (National Institute of Standards and Technology 2022) NIST 800-218 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf> accessed 13 February 2023.

[52] National Institute of Standards and Technology, 'Privacy Framework' (*NIST*, 8 January 2020) <https://www.nist.gov/privacy-framework/privacy-framework> accessed 17 January 2023; National Institute of Standards and Technology, 'NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management' (National Institute of Standards and Technology 2020) NIST CSWP 01162020 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf> accessed 17 January 2023.

[53] OWASP, 'Software Assurance Maturity Model' (n 47) 11.

[54] ibid 14.

[55] ibid 84.

[56] ibid 11.

[57] The 'CIA triad' refers to three major principles of cybersecurity: (i) confidentiality, (ii) integrity, and (iii) availability. Relevant sources covering the CIA triad include: Paul C van Oorschot, *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin* (Springer International Publishing 2021) 3; Wilson (n 5) 11; Urgessa (n 23) 3; Jeff Kosseff, 'Hacking Cybersecurity Law' (2020) 2020 University of Illinois Law Review 811, 831; Jeff Kosseff, 'Defining Cybersecurity Law' (2017) 103 Iowa Law Review 985, 997.

[58] In addition to the CIA triad, the computer scientific literature also seeks recourse to the 'privacy triad'. Similar to the CIA triad, this model includes three key factors for the protection of personally identifiable information and the management of that information: (i) unlinkability, (ii) transparency, and (iii) intervenability. Consider, among others, Marit Hansen, Meiko Jensen and Martin Rost, 'Protection Goals for Privacy Engineering', *IEEE Security and Privacy Workshops* (2015) 160; it is worth noting that other authors put forward similar views on this topic, albeit while using different terminology (i.e., predictability, manageability, and dissasociability): Sean Brooks and others, 'An Introduction to Privacy Engineering and Risk Management in Federal Systems' (2017) NIST IR 8062 17 ff <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf> accessed 11 January 2023.

[59] Dag Wiese Schartum, '"Technical and Organisational Measures" - A Systematic Analysis of Required Data Protection Measures in the GDPR' in Jean Herveg (ed), *Deep Diving Into Data Protection* (Larcier 2021) 294.

[60] OWASP, 'Software Assurance Maturity Model' (n 47) 81 ff.

Table 1
Illustration of OWASP's Software Assurance Maturity Model. This table shows the 'Threat Assessment' activity, which consists of two streams that can be assessed to evaluate a firm's technical security posture.[a]

Maturity level	Stream A: Application Risk Profile	Stream B: Threat Modelling
Level 1 – Ad-hoc approach to security.	Perform a basic risk assessment to understand the likelihood and impact of an attack.	Perform best-effort, risk-based threat modelling using brainstorming and existing diagrams with simple threat checklists.
Level 2 – Security activities integrated into the IT system's development lifecycle.	Understand the risk for all applications in the organisation by centralising the risk profile inventory for stakeholders.	Standardise threat modelling training, processes, and tools to scale across the organisation.
Level 3 – Continuous improvement and measurement of security practices.	Periodically review application risk profiles at regular intervals to ensure accuracy and reflect the current state.	Continuous optimisation and automation of the threat modelling methodology.

[a] The presented table here offers a summary overview of these practices; interested readers are referred to the SAMM for a comprehensive overview of the specific activities and corresponding maturity levels: OWASP, 'Software Assurance Maturity Model' (n 47).

modelling[61] offers an essential approach to systematically identify and mitigate security and privacy threats in software architectures.[62] Once the security and privacy threats have been identified, their risk level needs to be assessed based on their probability of occurrence and estimated impact.

Security requirements. Security (and privacy) requirements need to be explicitly specified and incorporated into the system's design. Depending on the characteristics and intended purpose of the IT system, this step forces firms to think about the security and privacy features that are most valuable to their system.

Secure architecture. A system architecture specifies all the components and technologies that will be implemented in the system under development. When selecting these components and integrating them into the foundation of an IT system, security and privacy must be considered alongside any other design objectives. For instance, system engineers can draw on established security principles.[63] Among others, it is important to secure the *weakest link* in a system. Since an IT system is only as strong as its weakest component, it is particularly valuable to address the most egregious risks rather than those that are easiest to mitigate. Another security principle specifies the importance of *defence in depth*[64], which promotes a layered approach to risk management in combination with diverse defensive strategies. If one layer fails, security problems can still be prevented by other layers. In addition to these principles, common design patterns, security solutions, reference architectures, standards and frameworks should be used to further strengthen the security of the system architecture.

3.1.3. Implementation

Security must also be considered when IT systems are being built and deployed. Three aspects are worth emphasizing in this respect: a secure system build, a secure system deployment, and efficient defect management.[65]

Secure build. A system build is the process of creating a computer or network system by assembling hardware components, installing software, and configuring settings. These steps must be carried out in a way that prioritises security and protects against potential threats and vulnerabilities, for instance by including (automated) security checks such as SAST and DAST (static and dynamic application security testing). Moreover, it is relevant to not only consider the features of the IT system itself, but also any dependencies on third-party software. These dependencies can introduce additional vulnerabilities into the system, which is why they should also be considered when building an IT system.

Secure deployment. When an IT system is deployed (i.e., installed, activated, or updated), it is made available for use. These deployment processes should be fully documented and include security checks. For example, software, scripts, or other assets should be validated to ensure that they function correctly and have not been tampered with. Typical measures used in this respect are signature verification checks and rollback procedures in the event of integrity breaches. In addition, equal attention should be paid to the management of 'secret information' such as passwords, tokens, and configuration files.

Defect management. During development, security defects (i.e., "bugs") need to be collected, recorded, and analysed. If properly managed, they can be easily dealt with. Moreover, by tracking any identified defects, useful metrics and feedback can be derived to guide further decisions for the development project or the security assurance programme.

3.1.4. Verification

The software verification phase takes places next. This stage refers to the necessity to verify the effectiveness of any implemented security measures; a process that happens through validation and testing. In essence, the goal of this stage is to identify and remedy any vulnerabilities or misconfigurations in the IT system. Three separate components are identified: an assessment of the architecture, specific requirements-driven testing, and general security testing.[66]

Architecture assessment. Early in the design process, security requirements were defined, and security threats were identified. These have subsequently been taken into account when modelling the IT system's architecture. During this architecture assessment stage, the architecture of the IT system is validated by checking it against the specified security and compliance requirements. The purpose of this step is to verify that the architecture mitigates known security threats (i.e., generic threats as well as specific threats identified through threat modelling).

Requirements-driven testing. Defining specific security requirements (e.g., role-based access control) for a robust IT system is an important activity in the design phase. These requirements are used as input for subsequent development steps. Once requirement-specific security measures have been implemented, it is equally important to verify them through security testing and to confirm that all specified requirements are indeed met. In addition, misuse or abuse testing can aid in detecting unexpected design flaws.

[61] Adam Shostack, *Threat Modeling: Designing for Security* (Wiley 2014) 624 p.; Zoe Braiterman and others, 'Threat Modeling Manifesto' (*Threat Modeling Manifesto*, 17 November 2020) <https://www.threatmodelingmanifesto.org/> accessed 13 April 2023.

[62] Kim Wuyts, Laurens Sion and Wouter Joosen, 'LINDDUN GO: A Lightweight Approach to Privacy Threat Modeling', *2020 IEEE European Symposium on Security and Privacy Workshops* (2020) 302; Mina Deng and others, 'A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements' (2011) 16 Requirements Engineering 3, 4; Adam Shostack, 'Experiences Threat Modeling at Microsoft', *MODSEC@ MoDELS* (2008) 1.

[63] Consider, for instance, the ten secure software principles coined in the early 2000s by Viega and McGraw: John Viega and Gary McGraw, *Building Secure Software: How to Avoid Security Problems the Right Way* (1st edn, Addison-Wesley 2002) 91 ff.

[64] Colloquially known in risk management verbiage as the Swiss cheese model.

[65] OWASP, 'Software Assurance Maturity Model' (n 47) 136 ff.

[66] ibid 197 ff.

Security testing. Security testing is, in general, an indispensable activity and an essential aspect of IT system development. Automated security testing tools offer one way of probing the robustness of IT systems and have the notable advantage of being easily scalable to many and large applications. However, system-specific manual testing is also required to tackle more advanced bugs, which typically require profound knowledge of the application, the underlying business logic, and the broader system context. Combining both techniques—automatic and manual security testing—should minimise the risk of overlooking some vulnerabilities.

3.1.5. Operations

Once hardware, software, and platforms are up and running, security must be maintained throughout the operational life of these systems, which implies that IT systems must be resilient to disruptions (e.g., attacks) and responsive to changes. Three aspects are worth highlighting: managing incidents, managing the system's technical environment, and managing operational activities.[67]

Incident management. Even if everything went according to plan during the development stage, there is still a non-zero chance that security incidents will occur. Two aspects of incident management are critical: detection and response. The quicker a breach is detected, the quicker it is possible to respond and to limit damage to a minimum. Having processes in place to detect incidents is therefore essential. Furthermore, when a breach occurs, it is important to *immediately* respond. Therefore, processes must exist to define the roles and responsibilities of everyone involved, and staff must be trained accordingly to successfully perform their incident response roles.

Environment management. Technology evolves and new features and patches are regularly released for IT systems. To ensure compatibility, standard configurations are often not secure by default. It is therefore important to invest in configuration hardening, patching, and updating.[68]

Operational management. The overall management of security throughout the operational support period requires the adherence to foundational principles, the implementation of monitoring techniques, and the formulation of appropriate responses for safeguarding security and privacy. This extends not only to current IT systems, but also includes legacy system management and action plans for decommissioning systems.

3.2. Appropriate organisational measures

3.2.1. Organisational maturity levels

The word 'organisational' can be interpreted in one of two ways.[69] On the one hand, 'organisational' refers to modes of organisation i.e., entities, departments, or groups. Within these organisational units, it is customary to assign different roles, tasks, and responsibilities to each individual member of the unit. On the other hand, "organisational" also connotes the creation of order, the imposition of structure, and the adherence to certain patterns. When attempting to understand the meaning of organisational security measures, these different meanings should be read in conjunction with one another. A combined reading subsequently indicates that "appropriate organisational measures" refer to the framework of procedures and practices to define the overall organisation's direction to achieve its security and privacy goals.

Within the framework of OWASP's SAMM, organisational security measures are not constrained to one specific stage of the IT system development cycle. Instead, these measures—referred to by the notion of *governance*—are considered as an overarching facet of IT system engineering.[70]

3.2.2. Governance

The OWASP maturity model defines governance as "*the processes and activities related to how an organization manages overall software development activities*".[71] This includes, but is not limited to, security concerns that affect development processes as well as business processes at an organisational level. Similar to the other categories taken up in the SAMM, governance can be divided into three main security practices: strategy and metrics, policy and compliance, education and guidance.[72] Note that these practices are not typically implemented by software engineers but that they are put into practice at the business level of the organisation.

Strategy and metrics. It is both useful and necessary to pursue software security objectives through an efficient and effective plan of action. This can be achieved by setting clear objectives and by identifying parameters for measuring the effectiveness of security programmes (e.g., number of vulnerabilities identified and remediated, threat detection and response times, percentage of employees completing security training). Once this has been achieved, a strategic security roadmap should be drawn up and security efforts should be aligned with the identified success metrics. By extension, this means that organisations need to create and promote such plans, measure their success, and continuously improve them.

Policy and compliance. This element focuses on understanding and establishing compliance with legal and regulatory requirements. A distinction needs to be made between the organisation's internal policies, on the one hand, and standards and compliance objectives imposed by third-party requirements, on the other hand.

Education and guidance. To facilitate a strong security programme, staff need to be equipped with the right security skills to enable them to design and develop secure software. This educational dimension can consist of general security awareness training, technology-specific training, or standardised in-house training programs. In addition to training and awareness, security should be embedded in the overall culture of the organisation. This can be achieved by training "security champions" in each team, developing a centre of excellence to promote secure software, and actively contributing to a secure development community.

3.3. Measures proportionate to the security risks and implementation costs

It is not realistic to expect SMEs to match the level of security of multinational corporations. An important role is therefore reserved for a cost-benefits exercise, where the costs of cybersecurity measures are weighted against their benefits for the firm. Put differently, determining the appropriate nature of cybersecurity measures also calls for a consideration of proportionality: measures are appropriate when they are proportional to the security risks and the implementation costs. This implies that large-scale enterprises that process vast datasets consisting of sensitive personal data will be judged more harshly under the ATOM benchmark relative to a small, family-owned business that only stores customers' email addresses.[73]

[67] ibid 250 ff.

[68] Note that Article 8(2) of Directive 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1 introduced a legal obligation for traders of digital content or a digital service to provide consumers with updates—including security updates—necessary to keep the digital content or digital service in conformity with the underlying contract.

[69] Schartum (n 60) 295.

[70] OWASP, 'Software Assurance Maturity Model' (n 47) 16 ff.

[71] ibid 16.

[72] ibid 16 ff.

[73] Note, however, that an SME that fails to implement any security measures still exposes itself to liability claims and administrative fines following the occurrence of a data breach.

In any event, the proportionality dimension of cybersecurity measures underscores the importance of threat intelligence (e.g., are we aware of any perpetrators that are likely to target us?) and the proper identification of risks (e.g., what data and systems are most critical to our operations?).[74] A deeper dive into the applicable legal provisions subsequently reveals a divide between a risk component and an economic component. Once these two facets have been adequately demarcated, maturity models can be relied upon to assess the firm's security posture and define strategies to further strengthen it.

3.3.1. Risk assessment

Cybersecurity measures should be proportionate to the security risks that may might occur, which is why the ATOM benchmark calls for a risk assessment. For all intents and purposes, "risk" is understood as a function of a threat's likelihood of occurrence and its impact (i.e., risk = likelihood x impact).[75] The *likelihood*-factor requires little further explanation and simply reflects the probability of a particular threat occurring within an organisation. For instance, given the sensitive nature of data aggregated by healthcare or financial firms, it is plausible to assume that such firms are particularly vulnerable to cyberattacks and that it would therefore be prudent to adopt a heightened level of protection. The *impact*-factor indicates the severity of the consequences should a threat actually occur. Logic suggests that if the expected effects of a cyberattack are severe (e.g., damage to critical infrastructure), then such firms are bound to an elevated duty of care.

By means of this risk calculus, firms can determine the threat level associated with their specific business model. Secondarily, risk assessments also permit firms to determine their *risk appetite* (i.e., the extent to which firms are willing to accept that a particular threat actually occurs). Often, the willingness to accept risk is directly related to the costs of early risk mitigation. Another, more general finding from risk assessments is that risk scales with the criticality of systems. Highly critical systems (e.g., utility firms) typically face higher levels of risk and therefore require higher levels of protection.

There are many ways to perform risk assessments in practice, ranging from ad-hoc "guestimates" based on rough, educated guesses regarding the severity of impact and likelihood (typically classified as high, medium, or low) to very formal, quantified approaches to risk.[76] The OWASP Risk Rating Methodology sheds some more light on the underlying factors that affect the impact and likelihood of a threat.[77] For instance, *risk likelihood* is influenced by several threat agent factors and vulnerability factors. The former concern attackers' skill level, motive, opportunities to exploit, and group size, whereas the latter include the ease of vulnerability discovery, the ease of exploiting a vulnerability, awareness surrounding the existence of a vulnerability, and the degree to which intrusions can be detected. *Risk impact*, on the other hand, is influenced by a number of technical impact factors (e.g., the loss of confidentiality, integrity, availability, and accountability) as well as business impact factors (e.g., financial damage, reputation damage, non-compliance, and privacy violation).

3.3.2. Economic assessment

While the GDPR does not explicitly prescribe an economic assessment[78], cybersecurity literature suggests that considering the financial impact of ATOM can serve as another practical approach to determine whether cybersecurity measures are proportionate to their implementation costs.[79] The proportionality dimension thus arguably also permits firms to evaluate the cost-effectiveness of a particular security measure and prioritise investments into cybersecurity in a way that best aligns with their risk appetite.

In essence, the economic assessment of cybersecurity measures involves performing a cost-benefit analysis, where the costs associated with implementing cybersecurity measures are weighted against the expected return on investment of those measures.[80] The cost component in this assessment should not only consider implementation costs in the strict sense, but also maintenance expenses and costs associated with the need to periodically revise or update security measures.[81] Return on investment, on the other hand, can be expressed not only in positive terms, such as achieving legislative compliance, but also in negative terms, such as the avoidance of certain costs, including decreased expenses related to resolving security incidents.

It should be noted, however, that being a smaller firm does not entitle that firm to compromise on cybersecurity for purely financial reasons. Rather, the economic assessment permits organisations to approach cybersecurity strategically, potentially leading to the adoption of more 'affordable'[82] measures if the identified risks were to allow this to happen.[83] Conversely, if the threat assessment indicates an elevated level of risk—for instance due to the criticality of the assets that must be secured or the high credibility of certain threats—then more advanced solutions should be deployed.[84]

Overall, though, the cost-benefit analysis must strike a balance between the degree to which a security measure reduces risk and the degree to which a measure costs money. In any case, the economic calculus should be made with due regard to the organisational capabilities and

[74] It is useful to draw a parallel between the need for threat intelligence and the requirement under Article 35 GDPR to draw up a Data Protection Impact Assessment (DPIA). For a comparison between DPIA and threat modeling approaches, see Laurens Sion and others, 'DPMF: A Modeling Framework for Data Protection by Design' (2020) 15 Enterprise Modelling and Information Systems Architectures 1, 4 ff.

[75] Gary Stoneburner, Alice Goguen and Alexis Feringa, 'Risk Management Guide for Information Technology Systems' (National Institute of Standards and Technology 2002) NIST SP 800-30 8.

[76] A well-known example of a formal risk-based approach is the FAIR (Factor Analysis of Information Risk) model: X, 'Quantitative Information Risk Management' (*FAIR Institute*, 16 February 2023) <https://www.fairinstitute.org> accessed 20 February 2023.

[77] OWASP, 'OWASP Risk Rating Methodology' (*OWASP Foundation*, 15 October 2022) <https://owasp.org/www-community/OWASP_Risk_Rating_Methodology> accessed 20 February 2023.

[78] It should be noted, however, that the cost of implementing ATOM is now a factor to be taken into account under Article 21(1) of the NIS2 Directive.

[79] There is a large body of technical literature that addresses the economic dimensions of cybersecurity measures, providing economic models and theories to facilitate strategic decision-making when investing in ATOM; for an overview of the different strands, see Tara Kissoon, 'Optimum Spending on Cybersecurity Measures' (2020) 14 Transforming Government: People, Process and Policy 417, 419–420; especially known for their research on the economics of cybersecurity are Lawrence A Gordon and Martin P Loeb, 'The Economics of Information Security Investment' (2002) 5 ACM Transactions on Information and System Security 438, 440, who write that the optimal amount to spend on cybersecurity does not exceed 37% of the expected loss; Lawrence A Gordon, Martin P Loeb and Lei Zhou, 'Investing in Cybersecurity: Insights from the Gordon-Loeb Model' (2016) 7 Journal of Information Security 49.

[80] Bruno Rodrigues and others, 'SEConomy: A Framework for the Economic Assessment of Cybersecurity' in Karim Djemame and others (eds), *Economics of Grids, Clouds, Systems, and Services* (Springer International Publishing 2019) 160: "*A rational approach in defining what is 'appropriate' involves (a) identification of risks by examining potential vulnerabilities and their chances of a successful exploitation, (b) the cost of these results if vulnerabilities are exploited, and (c) the cost of mitigating vulnerabilities*".

[81] See Thomas A Johnson, 'Economic Cost of Cybersecurity' in Thomas A Johnson (ed), *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare* (Taylor & Francis 2015) 262, who identifies two 'cost streams' pertaining to cybersecurity, notably internal costs (e.g., detection, containment, recovery, etc.) and external costs (e.g., information loss, business disruptions, equipment damage, etc.).

[82] E.g., firewalls, anti-malware software, and basic network security controls.

[83] Hofman (n 25) 52.

[84] E.g., automatic threat detection methods, penetration testing, and data loss prevention tools.

the financial health of the organisation in question. Yet, while the economic assessment allows for the selection of more affordable measures—severity of the identified risks permitting—it cannot serve as a justification for falling below the threshold of providing an adequate level of security.[85]

4. Effects of (in)appropriate cybersecurity measures

The main and most problematic consequence of inappropriate cybersecurity measures is the insecure state of the IT system, which exposes the system to security breaches and various other risks (e.g., unauthorised access or data leakages). Besides any technical risks caused by the inadequate implementation of security and privacy-by-design practices, legal liability must also be considered.

Determining liability for cybersecurity incidents is a complex, yet critical step in ensuring that firms internalise the implications of security breaches and, thus, adopt appropriate cybersecurity measures.[86] Following a cybersecurity incident, affected parties typically seek recourse before a court of law to obtain a suitable remedy. Here, appointed judges[87] must review any adopted cybersecurity measures against a liability standard[88], which in the EU is centred around the ATOM benchmark and the requirement to attain an appropriate level of security in relation to the risks posed.[89]

Undertakings are thus subject to a *duty of care* when implementing cybersecurity measures (i.e., the means) and must, in any case, attain an appropriate level of security relative to the identified risks (i.e., the end result).[90] The converse side of these two obligations is that data subjects are entitled to a reasonable expectation[91] that any processing involving their personal data is carried out with due respect for the confidentially and integrity of those data. Consequently, the analysis of cybersecurity measures yields the following litmus test: *did the firm in question proceed with reasonable caution as any other prudent firm would have done under the same circumstances*?[92] Answering this question can lead to one of two possible outcomes:

(i) *A firm has taken appropriate cybersecurity measures and has ensured a level of security appropriate to the risk, but a security breach occurs nonetheless.* In these circumstances, the firm is deemed to have met the ATOM standard and is therefore not found to be negligent.[93] The data breach is qualified as *not attributable* to the firm, and the firm in question is likely to escape tortious liability as well as, in most[94] cases, contractual liability.

(ii) *A firm has* not *taken appropriate cybersecurity measures and therefore has not ensured a level of security appropriate to the risk, and a security breach occurs.* In this scenario, the firm is found to be negligent by having failed to meet the ATOM standard.[95] The occurrence and consequences of the data breach are thus *attributed to* a negligent attitude on behalf the firm. A violation of the confidentiality and integrity principles are likely to be found and the firm faces liability.

When contemplating about this legal test, it is useful to keep in mind that cyberattacks can never be completely ruled out. From that perspective, reference should be made to the Latin maxim *impossibilium nulla obligatio est* (meaning, no one is held to the impossible). The more practical implication thereof is twofold. On the one hand, no security measures can guarantee absolute security, and this is why the prevention of cybersecurity incidents is likely to be qualified as an *obligation of means*. Hence, even if a security breach occurs, this does not necessarily indicate that the measures were not appropriate at the time of their implementation or that the level of security was not appropriate to the risk.

On the other hand, there is a direct link between the cybersecurity measures to be adopted and the result to be attained. As Hofman writes, security measures must always be appropriate in light of the concrete risks posed by the processing of personal data, and this arguably represents an *obligation of results*.[96] After all, the ultimately goal is the prevention of cybersecurity breaches. This combined approach—accepting that cybersecurity breaches can never be completely ruled out and that the fundamental rights of data subjects mandate a high level of cybersecurity—implies that organisations cannot resort to blindly implementing cybersecurity measures, but that they must select measures that are commensurate with the level of risk. Put another way, the direct means-end relationship between the appropriateness of the measures and the appropriateness of the level of security ensures that the adoption of ATOM cannot be seen as a mere box-ticking exercise.

5. Conclusion

Other scholars have noted that "*the only constant in cybersecurity is change*".[97] This particular message resonates well with the current contribution. In some ways, the tangible benefits that IT systems bring to our daily lives can hardly be denied. Yet, with IT being so prominently present in our lives, the role and importance of cybersecurity should not be overlooked. Security threats always lurk around the corner, which is why IT products, services, and infrastructure must come equipped with appropriate technical and organisational security measures.

While each firm's approach to cybersecurity is unique, *resilience* is a key value that should always be pursued. Cybersecurity is therefore not to be understood as a one-off, set-and-forget intervention. Instead, it requires *defence in depth* and calls for a well-though-out *action plan* to cope with intrusions. On balance, the goal of appropriate cybersecurity

[85] Hofman (n 25) 52.

[86] Eldar Haber and Tal Zarsky, 'Cybersecurity for Infrastructure: A Critical Analysis' (2017) 44 Florida State University Law Review 515, 555.

[87] Judges may designate IT experts to produce expert evidence in the course of legal proceedings. These experts intervene in the proceedings to guide judges in their deliberation processes.

[88] Haber and Zarsky (n 87) 555.

[89] See above at Section 1.

[90] Eric Tjong Tjin Tai and others, *Duties of Care and Diligence Against Cybercrime* (Tilburg University 2015) 53; OECD, 'Enhancing the Digital Security of Products: A Policy Discussion' (2021) OECD Digital Economy Papers No. 306 22; in the context of insecure software: Pieter Wolters, 'The Obligation to Update Insecure Software in the Light of Consumentenbond/Samsung' (2019) 35 Computer Law & Security Review 295; apropos IoT devices, consider: Rolf Weber, 'Liability in the Internet of Things' (2017) 5 Journal of European Consumer and Market Law 207, 210.

[91] Matthew Channon and James Marson, 'The Liability for Cybersecurity Breaches of Connected and Autonomous Vehicles' (2021) 43 Computer Law & Security Review 1, 9.

[92] Cf., Weber (n 91) 212, who equally draws from the bonus pater familias criterion.

[93] Stanislaw Piasecki and Jiahong Chen, 'Complying with the GDPR When Vulnerable People Use Smart Devices' (2022) 12 International Data Privacy Law 113, 129; Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130, 157.

[94] From a purely contract law perspective, this is, of course, somewhat short-sighted and more information is needed vis-à-vis the contractual structure to formulate clearer answers. Among others, the answer to the contractual liability question will depend on whether the firm was subject to an obligation of means or an obligation of results.

[95] Piasecki and Chen (n 94) 129.

[96] Hofman (n 25) 301–304.

[97] Urquhart and McAuley (n 30) 452; Weber and Studer (n 2) 728.

measures is, firstly, to prevent cyberattacks whenever possible and, secondly, to have a contingency plan in place to repress such events if they do occur. These two tasks are directly related to reaching a specific end result, which is to ensure an appropriate level of security.

In determining the appropriateness of cybersecurity measures, reference should be made to *cybersecurity maturity models*. Such models permit firms to analyse their specific cybersecurity policies against several reference maturity levels while taking the firm's financial and operational capabilities into account. An important take-away of such models is that security measures should be tailored to and scale with the size and scope of activities of the firm in question. Moreover, the appropriateness of cybersecurity measures features a strong temporal dimension: any adopted measures must stand the test of time, meaning that an IT system must not only be safe at the time of being put on the market, but also throughout its lifecycle. Among other, this entails a requirement to regularly review and update cybersecurity measures.

Before concluding this contribution, a final, closing observation should be made: the threat of liability should not be the sole motivator for firms to put appropriate cybersecurity measures in place. Instead, firms should find themselves incentivised to secure their IT systems at their own discretion, in order to protect their own assets, data, and by extension, commercial interests. Put differently, being serious about privacy and security is also a matter of demonstrating respect towards end users, which can yield a compelling advantage in competitive markets.

The topic of cybersecurity is neither going to disappear nor diminish in importance in the future. Several new legislative initiatives—such as the recent entry into force of the NIS2 Directive[98], the proposed Cyber Resilience Act[99], the Digital Operational Resilience Act[100], and safe harbour rules on ethical hacking[101]—attest to this. If anything, it becomes apparent that cybersecurity is increasingly having horizontal effects i.e., it creates obligations between private parties. With liability hanging in the balance, the importance of transitioning from technical insight to legal compliance cannot be overstated.

CRediT authorship contribution statement

Christof Koolen: Conceptualization, Methodology, Writing – original draft, Writing – review & editing. **Kim Wuyts:** Methodology, Writing – original draft, Writing – review & editing. **Wouter Joosen:** Supervision, Project administration. **Peggy Valcke:** Supervision, Project administration.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

This work was supported by a grant of the Research Foundation Flanders (FWO) [grant number 11G0920N], is partially funded by the Research Fund KU Leuven, and by the Flemish Cybersecurity Initiative Flanders. The authors are grateful to dr. Mariano Di Martino and dr. Tom Hick for providing valuable input on the draft version of this paper. All remaining errors are our own.

Christof Koolen works as a Ph.D. researcher at the Centre for IT & IP Law (KU Leuven, Belgium). He holds a Master of Laws from the KU Leuven and a Magister Juris degree from the University of Oxford. He conducts research on the legal implications of smart devices within the EU internal market.

Kim Wuyts is a senior postdoctoral researcher at the imec-DistriNet research group at the department of Computer Science (KU Leuven, Belgium). She holds a Master of Engineering in Computer Science from the KU Leuven. Her research predominantly focusses on privacy engineering and privacy threat modelling.

Wouter Joosen is a full professor at the Department of Computer Science (KU Leuven, Belgium), where he teaches courses on software architecture and component-based software engineering, distributed systems, and the engineering of secure service platforms. His research interests include security and privacy of distributed software systems, services, and applications.

Peggy Valcke is a full professor of Law & Technology at the Faculty of Law & Criminology (KU Leuven, Belgium). She is a co-director at the Centre for IT & IP Law and a principal investigator in the Security & Privacy Department of imec. Peggy's current research focus lies with the rise of artificial intelligence technologies, and in particular algorithmic decision-making.

[98] Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (n 11).

[99] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 [2022] COM(2022) 454 final.

[100] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector [2022] OJ L 333/1.

[101] Article 2(j) juncto Article 8, Loi sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé [2022] Moniteur Belge 97213.