European Commission

JRC TECHNICAL REPORT

Information security in the age of EU-Institutions digitalisation, a landscape analysis

KAMBOURAKIS, G.

NEISSE, R.

NAI-FOVINO, I

2021

Joint Research Centre

EUR XXXXX XX

EU Science Hub
https://ec.europa.eu/jrc

JRC125214

Ispra: European Commission, 2021

How to cite this report: KAMBOURAKIS, NEISSE, NAI-FOVINO, *Information security in the age of EU-Institutions digitalisation, a landscape analysis*, European Commission, Joint Research Centre, 2021, JRC125214.

Contents

Abstract

The galloping digitisation, cloudification, and the so-called “new norm” introduced by the pandemic along with the increasingly hostile cyberspace brought new, and in some cases, unforeseen challenges to EU institutions, bodies, and agencies (EUIBAs). This situation is further complicated due to the new missions assigned to several of these entities, including defence funding, border management, and foreign direct investment screening. Undoubtedly, this rapidly evolving ecosystem leaves no room for complacent regarding information security. Namely, just a quick contemplation on this ever-changing and complex digital landscape, the emergence of new tasks, and the many-to-many fashioned synergies developed among EU entities, is more than enough to demonstrate the necessity for creating and ratifying a contemporary common baseline for information security across EUIBAs. For instance, new missions assigned to EUIBAs will eventually create greater demands for handling and exchanging large volumes of information and data for which it is possible that no classification has been set and no rules on how to exchange and store them exist. Altogether, these developments affect all the involved parties, and immensely render the need for the establishment of a unified and harmonised information security framework more imperative than ever. Such a framework is anticipated to decisively contribute to the secure handling and exchanging of any sort of information, either digital or not. Moreover, at least in the mid-term, the fruits of this endeavor are expected to also diminish the overall attack surface, as everyone will follow the same rules, and personnel training can be coordinated and harmonised, let alone the reduced associated resources and management costs.

The report at hand offers a fresh and detailed perspective on the aforementioned challenges, but interestingly from an information risk assessment viewpoint. Specifically, the focus is on any piece of information, both classified, and non-classified, including that stored or managed by third-party providers on behalf of the Commission and it is extended to digital archives and across the whole information lifecycle. We generally follow ISO/IEC 27005:2018, where risk assessment splits into three basic phases, namely, risk identification, risk analysis, and risk evaluation. Furthermore, the report offers generic risk treatment actions as guidelines for mitigating the identified risks. Risk assessment on the assets of interest is basically done in a high-level, coarse-grained rather than technical low-level and exhaustive way. For this reason, risk analysis is based on a qualitative approach, and it is also merged with risk evaluation. The report aspires to not only serve as a means to stimulate and facilitate the needy process towards a new EUIBAs policy addressing common rules on Information security, but also as a reference to anyone interested in better understanding the diverse facets of this fast evolving and thought-provoking ecosystem.

1 Introduction

Information security focuses on the confidentiality, integrity, and availability of information, and it is concerned with any kind of information either digital or analogue, material or immaterial [1]. Put simply, information security pertains to the processes and methodologies which are developed and put in action to safeguard printed, electronic, or any other form of classified information or data from unauthorised access, use, misuse, disclosure, modification, destruction, or disruption. Naturally, today, information security should also take into consideration a cybersecurity perspective, focusing on cyberspace and cyberassets[1], and as such, has to sit also on top of every "cyber thing" which is potentially vulnerable via Information and Communication Technology (ICT), including objects like cars, traffic lights, unmanned aerial vehicles, embedded processors and controllers, and so on.

Nowadays, the number of Information and Communication Technologies (ICT) systems, cloud services and connected devices is constantly augmenting at an increasingly, if not frantic, pace. With the advent of 5G and beyond networks and the rise of Internet of Everything (IoE), the number of connected devices and systems will explode shortly. In the context of any organisation and in conjunction with the proliferation of e-services, these developments lead to big data of various levels of sensitivity and all this information must be protected somehow. And while not all data or information is equally sensitive from a confidentiality viewpoint, it may call for protection from the perspective of integrity (correctness) and traceability. That is, on the one hand, one needs to have guarantees that the information is intact, and on the other to be able to verify that the information is indeed stemming from the legitimate source. And on top of everything else, all the stored information and data should be always and readily available via the underlying services.

Organisations' information resides no longer in air-gapped networks, but in networks that almost every employee can access. Due also to the COVID-19 pandemic, teleworking is now both a necessity and a worldwide trend, but this places major demands on how information is kept, handled, and exchanged. And while a great mass of resources is devoted to contemporary and sophisticated technical safeguards, the employees must also be well-informed and mindful of the risks to properly utilise the available protections. Namely, irrespective of the technical safeguards, which undoubtedly protect from technical attacks, social engineering still remains the most effective way of penetrating the defences and granting unauthorised access to the organisation's assets. Besides, digitalisation widens the window of opportunity to any opponent. From individuals, groups and organisations who seek the monetisation of stolen data, those who wish to eavesdrop on information, those who aim to harm the targeted entity, to those who just want to show off and feed their ego. At all events, threats to information are of diverse kinds and pervasive; kidnapping information by means of encrypting it, monetising on information stolen via espionage, gaining access to specific classified information, paralysing e-services and websites through a Distributed Denial of Service (DDoS) attack, and so on.

In this context, information security is far from being characterised as straightforward and effortless. Instead, along with cybersecurity, it is a multifaceted, and rapidly changing ecosystem, which involves and is affected by the simultaneous interaction of several factors, including people, processes and technology, and the myriad of applications and services in the IoE. All these factors are tightly or loosely interconnected by means of the underlying physical and communication infrastructure, either wired or wireless. Today, more than ever, information security and cybersecurity in general, in the context of any organisation, country, union of states, and even globally, is a prerequisite for competence. Particularly for the European Union (EU), this necessity has been, among others, already documented in JOIN/2017/0450 [2] and EU directive 2016/1148 [3].

At the same time, the cyber threat landscape is increasingly hostile. As reported by CERT-EU [4], the number of major attacks on EU institutions, bodies and agencies (EUIBAs) was on the rise during the third quarter of 2020, while ransomware remains the most significant cybercrime threat in Europe. In this context, EUIBAs need to constantly evaluate and revise their information security framework and decision-making procedures for considering and tackling these threats. Indeed, the Security Union

[1] Anything that has value to an individual, an organisation or a government" [1].

Strategy adopted by the COM [5] in July 2020 caters for the adoption of common rules for all EUIBAs on information security and cybersecurity.

That is, nowadays, the zero-risk philosophy has been proven unrealistic, hence any type or size of organisation must follow a formalised approach for the identification, assessment, management, and communication of risk in the cyberspace.

In fact, this requirement is specifically defined in ISO/IEC 27005:2018 [6], where information security risk assessment comprises three distinct, but closely interrelated phases, namely risk identification, risk analysis, and risk evaluation.

1.1 Rationale and scope of the report

Under the prism of the increasingly hostile cyberspace and the challenges posed by galloping digitisation, cloudification, and the "new norm" introduced by the pandemic, creating a common baseline for information security, across EUIBAs will greatly contribute to the secure handling and exchanging of any sort of information, either digital or not. In the mid-term, this also reduces the attack surface, as everyone follows the same rules, and personnel training can be coordinated and harmonised. Moreover, this strategic aim works in favour of abolishing the need - along with the associated resources and management costs - for creating and maintaining custom-tailored, diverse, and sometime ad-hoc security rules, which eventually augment fragmentation and complexity, decrease interoperability, and leave room for shortcuts and misconstructions.

From this perspective, the present report aims at performing a high-level risk assessment on the core information assets and relevant procedures that pertain to EUIBAs. As detailed in section 2, among other reasons, this necessity mainly stems from the rapid digitalisation, cloudification, externalisation, and sometimes fragmentation of the underlying information management procedures, such as exchanging, storing, , destroying data, which in terms of information security, call for revision and unification across all the involved parties. This argumentation is also strengthened by the fact the EU ecosystem has been significantly evolved in terms of the type and volume of information that is processed. For instance, the growth of defense related and border control related activities leads to more exchanges of classified information. The same trend applies to the area of financial activities. This comes on top of areas where there is a long history of dealing with sensitive files, such as trade or competition.

In this respect, the focus of this report is on all information, both classified (EUCI), and non-classified. This also includes all information stored or managed by third-party providers on behalf of the Commission and it is extended to digital archives and across the whole information lifecycle.

Where applicable, and to some extent, the report also covers (i) procedures to govern access to the relevant information by staff, including clearance procedures, access to facilities, and online meetings, (ii) systems handling classified information and processes, mechanisms for the certification of cryptographic products within the EU, (iii) governance structures and mechanisms in charge of governing a secured information exchange within EUIBAs and to ensure mutual trust in handling of information between parties, (iv) procedures to ensure proper encryption of information across EUIBAs, depending on its level of sensitivity, (v) security investigation in the context of an EUCI breach, (vi) awareness raising and training on information security, (vii) counter intelligence and counter terrorism activities, in relation to risks of eavesdropping, spying and interception of information, and (viii) identity management related issues across institutions, including registration, authentication, and so on.

Risk management for items like IT assets in general, physical security (building and facilities), business continuity and disaster recovery, and intellectual property protection of information, lie outside the scope of the current report.

1.2 Methodology

For the needs of this report, we generally follow ISO/IEC 27005:2018, where, as already mentioned, risk assessment splits into three phases, namely, risk identification, risk analysis, and risk evaluation. On top of that, we propose generic risk treatment actions as guidelines for mitigating the identified risks. It is to be noted however that given the readership of the report, risk assessment on the assets of interest is mostly done in a high-level, coarse-grained rather than technical low-level and exhaustive way. For this reason, risk analysis is based on a qualitative approach rather than a quantitative or hybrid one, and it is also merged with risk evaluation in the same subsection. Lastly, for the threat analysis process, we rely on "The security cards" security threat brainstorming toolkit [7].

1.3 Structure of the report

The next section focuses on the risk assessment process, exploring the current context and the associated trends that justify the need for a new policy addressing common rules on Information security. It also delves into the various steps of risk identification and elaborates on risk analysis and evaluation. The last section concludes.

2 Risk assessment

Before delving into the specifics of the risk assessment process for EUIBAs, it is important to understand risk in the context of information security. Like any other type of risk, information security risk is the combination of two main factors: (a) how likely a negative security event is to happen, and (b) the potential consequences of such an event. Even if an event is not likely but its impact is large, the resulting risk may still be critically important. For example, this is the case when the outcome of a terrorist attack can put human lives at risk, albeit the chances of it occurring might be generally low. Even in very unlikely threat scenarios, the risk still needs to be properly assessed and addressed. Generally, the likelihood that a negative event will take place depends on who might be motivated to conduct the attack and on how the attack could take place. The impact is the consequence of a successful attack on the target.

Information security risk is based on a triad of factors: (a) threat actors, i.e., attackers, (b) vulnerabilities, i.e., systemic weaknesses, and (c) impacts, i.e., adverse effects of a successfully carried out attack, either intended or collateral. Figure 1 puts these three dimensions of information security into context, showing their interconnection and their role in the composition of the information security risk. As observed from the figure, there exists a clear interaction between all these three dimensions, depicted by the innermost clockwise circle of arrows. Specifically, as detailed in this section, threat actors refer to any actor or group with a motivation to carry out an attack to achieve a certain reward. This can include the full spectrum from mere cyber criminals who seek to make money, to activists following an ideology, or to state-sponsored attackers.

Threat vectors on the other hand are the means at the disposal of threat actors to exploit existing vulnerabilities by using a threat tool to realise an attack. For instance, any form of malicious software, also known as malware, can be considered as a threat tool. Vulnerabilities can take on many forms, but mainly reflect security weaknesses in the design of software, hardware, or processes. It is also clear that threat actors seek to receive a reward from their attack, ultimately causing the impact. The attack impact is typically caused by a combination of rewards intentionally sought by the adversary, say, money stolen by a banking Trojan, and collateral damage of the attack, say, a ransomware attack that results in the disruption of communication networks. The area within the three overlapping circles of Figure 1 represents the effective information security risk. In theory, no risk exists if one of the three key elements is absent. Likewise, the risk is greatest if all three factors are high at the same time.

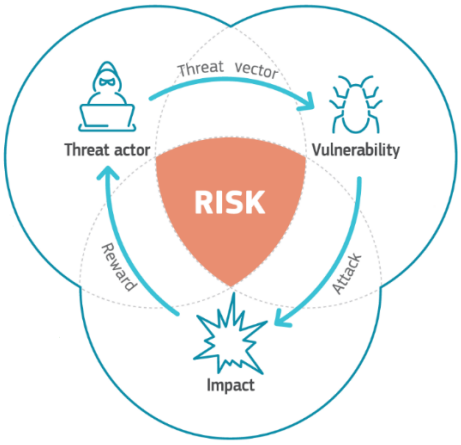

Figure 1. *Risk conceptual model*

In a more detailed approach, depending on the focus of interest, namely, uncertainty, impact, probability, etc., the literature provides several definitions of the concept of risk [8], [9]. For instance, according to NIST [10], the terms *"risk"* and *"information system-related security risk"* are defined as "*A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs;*

and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation". From this definition, it is straightforwardly inferred that ICT-related security risk is the intersection of likelihood (probability) and severity of impact (consequences), where likelihood is typically determined from threat[2] and vulnerability[3] factors.

Consequently, to aid decision making as depicted in Figure 1, information security risk can be abstractly quantified as a function of threat, vulnerability, and impact[4].

Naturally, risk can never be eliminated, so the result of the formula is always greater than zero. Generally, it can be said that threats on assets are materialised via attacks (threat events), which exploit vulnerabilities that have not been eradicated or mitigated with appropriate controls (countermeasures).

Put simply, risk can be defined as the potential for abuse, damage, or destruction of an asset because of a threat exploiting a vulnerability.

Common categories of threats in the information field are physical damage (fire, corrosion, dust, flood, etc.), compromise of information (passive or active eavesdropping, information tampering or disclosure, privacy violations, etc.), unauthorised actions (illegal processing of data, unauthorised use of equipment, etc.), just to mention a few. By using the previous abstract formula, one can practically quantify or qualitatively describe the risk level on a given asset.

For example, what is the risk profile of an employee using a laptop to store important business information that must not be disclosed outside the organisation? Roughly, in a scale of low, medium, and high, one can estimate likelihood to be, say, medium (the employee may lose the laptop, having the information disclosed to unauthorised parties), and impact to be high (important information may be disclosed to unauthorised parties, breach of law regarding data protection, the organisation may by subject to financial penalties, etc.). On the other hand, having the laptop's disk encrypted it may reduce the impact to an acceptable level.

It is therefore clear that, depending on the context, the contributing factors in the abovementioned risk formula must be clearly defined, assessed, and quantified through a proper security risk assessment process, which is illustrated in the upper part of Figure 2. This ensures that the information risk can be understood in a reliable, consistent, and formalised manner. Indeed, developing an information security policy is the keystone of security risk management. People need guidance on how to interact with the information, services, and devices around them. Namely, the security policy offers the statement of objectives and intents that the information security infrastructure is designed to materialise. Putting it another way, having a well-defined and not overly complex policy at hand, one can know what to do, and follow the required steps to ensure that the defined goals are reached.

Simply stated, information security risk management refers to the balancing of costs and benefits, i.e., the cost-benefit trade-off associated with any security decision. It is to be noted however that risk perceptions that drive risk management in general often change among the stakeholders. For instance, it is true that employees' views regarding information risk are perceptive and less formal and accurate than those of security experts. Nevertheless, such opinions may lie on legitimate concerns that are normally neglected from risk assessments conducted by experts. Therefore,

[2] The *"potential cause of an unwanted incident, which may result in harm to a system, individual or organization"* [1].
[3] A *"weakness of an asset or control that can be exploited by a threat"* [1].
[4] This should be regarded as a risk conceptualisation model rather than a mathematical equation. In the literature, there are also other similar equations for approximating risk, including Risk = *f(value of damage, likelihood of threat attempt, likelihood of successful threat execution)*, *Risk = f(vulnerability, threat, asset value, probability of occurrence)* and *f(threat, vulnerability, asset value, possibility of detection)*, while others even add an extra factor called "level of uncertainty".

insiders' and sometimes public feedback may be a key factor for recognising risk factors, even if it is not taken into account when assessing the potential impacts. Moreover, in the presence of conflicting values or goals, such opinions, can offer credible judgement regarding the trade-offs. In this respect, policy makers should be also aware of laypeople's views of risk and concerns and consider them as a valid input into security risk management and regulation.

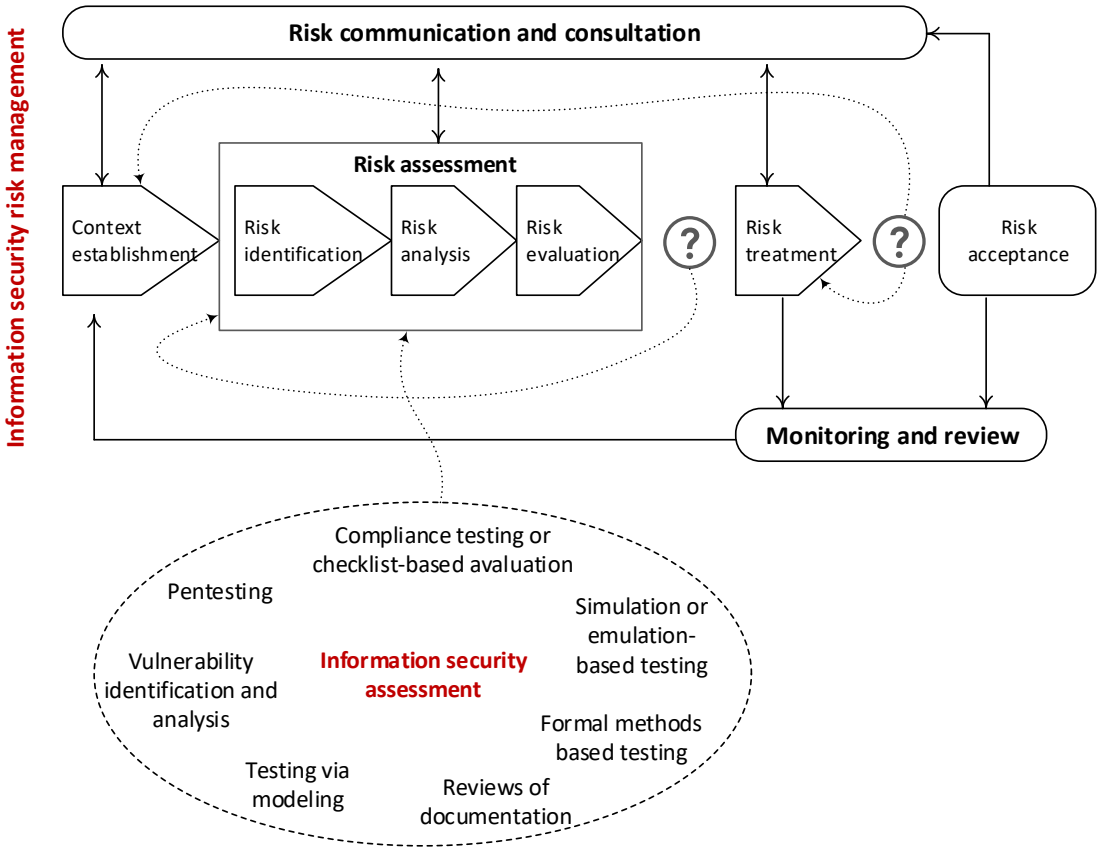

Figure 2. Information security risk management process (adapted and complemented from [6]).

It is important to make a distinction between the concepts of information risk assessment and information security assessment. As shown in Figure 2, while these tasks are somewhat interrelated, they are not identical. Precisely, the goal of information security assessment, typically conducted via passive or active testing, examination, or interviewing, is to determine the current information security posture of the assessed entity, namely a process or a device, and ascertain whether that entity satisfies specific predetermined security objectives [11]. Information security assessment embraces different methods, including penetration testing, compliance testing often based on checklist evaluation, vulnerability identification and analysis, testing via modelling, simulation or emulation-based testing, and formal analysis, and hence it is mainly related to the risk identification phase of the risk assessment process.

Naturally, in the real world, vulnerabilities always exist as no ICT system nor any organisation, especially the multilevel and inter-governmental ones, is perfectly secure, nothing is without impact and there will always be some motivation for threat actors to attack a system. Thus, the goal of an information security risk assessment is to determine the magnitude of risk, not whether it is present or not.

If the estimated risk warrants action, considering the available resources, mitigation strategies (controls) need to be devised to reduce that risk to an acceptable level. Namely, as detailed in subsection 2.4, information security risk can be mitigated either by deploying mechanisms aimed at reducing the information security threats, i.e., deterrent actions, including cybercrime prosecution, by preventing vulnerabilities, or by mitigating the effect of impacts, i.e., increased resilience. The level of

risk acceptance is often combined with another aspect of risk management, namely, the transferal, i.e., the contractual shifting of a risk from one part to another through insurance.

The rapidly unfolding digital transformation constantly creates new digital assets, which can be vulnerable to attacks, thereby increasing rewards and motivations for threat actors. This enlarges the so-called attack surface, ultimately leading to higher potential impacts, and therefore calls for prompt adaptations in the organisation. Nevertheless, information security risk can also be contained by putting in place the right countermeasures at the technical, organisational, and societal levels. For instance, such countermeasures may spread along both the management and technical axes and include the establishment of common terminology and practices about information security, the definition of formal cooperation procedures, the use of common security tools, the specification of harmonised teleworking and digital workplace rules, the employment of a common approach on identities, and so on.

2.1 Context establishment for EU organisations

The increasing digital transformation of EUIBAs, brings new information security challenges. These challenges are an immediate consequence of the fast-paced and high-scale digital transformation that is in general driving developments in Europe, but also worldwide. The digital transformation thrives on the application of new technologies with the goal of improving the daily life of citizens and, with respect to EU entities, enabling a more efficient European public administration. The positive trend for new and improved services does not apply only to citizens, but also to the administration per se. Several EU entities are assigned new complex and multi-dimensional tasks that also yield big data and information of various types and classification levels. On top of challenges already faced due to the digital transformation, the new norm created recently by the COVID-19 pandemic made it even more difficult to ensure the protection of the information within the EUIBAs. This new norm includes the large-scale decentralisation of the workforce, without physical presence, and massive adoption of online digital services for coordination and collaboration.

From an information security and privacy viewpoint, the information generated and handled by the plethora of services is of diverse types and levels of sensitivity. For instance, one can discern among financial, draft legislation, politically sensitive information, security-related information, information used in investigations, employee records, personal data, scientific publications, website content, etc. The sensitivity of data belonging to each category, but also that within the same category may also vary. For instance, with reference to [12], EUCI fall into four classes, namely Top Secret, Secret, Confidential, and Restricted. Certain EU organisations can also distinguish between levels of non-classified information based on their particular confidentiality needs, so a certain degree of diversity, which in turn may reduce interoperability, does apply. It is therefore obvious that the underlying information security measures must not be monolithic, rather they should be directly associated to the particular case and the kind of information they protect. For instance, employee data should be treated as personally identifiable information (PII), while information used in investigations is typically kept confidential. And naturally, IT services are only one way in which information is handled; manual procedures also apply, although in a gradually lesser degree. Hence, information security should be carried out in a holistic way. Finally, a certain balance between transparency and security should be maintained, Namely, is there a straightforward way to make access to public records easy for citizens, while using controls that protect data from attackers?

Having the above in mind, the goal of this subsection is to sketch the current context in which the EU administration operates, and summarise the information security challenges faced today by EU organisations, which in most cases have been intensified by the “new norm” because of the COVID-19 pandemic.

In the light of the anticipated proposal for a regulation establishing common information security rules for all EUIBAs, these challenges can be organised in four main categories:

1. New challenges faced by EU entities because of new tasks assigned to them.

2. New challenges faced by EU entities because of the digital transformation.
3. New challenges to be dealt by EU entities because of the “new norm”.
4. Shared challenges that are amplified due to the lack of common information security rules.

A detailed discussion around these categories of challenges is given in the following subsections.

2.1.1 New tasks assigned to EUIBAs

Information security policies and practices should be adjusted to the new tasks assigned to EUIBAs. Examples of such tasks include defence funding, border management, and foreign direct investment screening as described in COM(2021) 70. For instance, according to Regulation (EU) 2019/1896, article 9, a specific capability development planning process has been established for EU integrated border management. This will pave the way for the coordination of Member States’ national capability development plans related to border management and FRONTEX’s own capability plans. On the other hand, Regulation (EU) 2019/452 establishes a framework for the screening of foreign direct investments into the Union, which when implemented “can help to safeguard critical technologies and infrastructure in a way that also benefits EU operators that rely on them”.

Nevertheless, these initiatives and tasks go hand in hand with new challenges regarding information security. That is, following these synergies among civil, defence, and space industries, new demands will eventually arise in terms of handling and exchanging a large volume of information and data for which it is possible that no classification has been set and no rules on how to exchange and store them exist. This naturally affects all the involved parties, and immensely renders the need for the establishment of a unified and harmonised information security framework more imperative than ever.

2.1.2 Digital transformation

Nowadays, the information security challenges faced by the EU administration is a direct consequence of the digital transformation of the European society, the growing tendency on e-government (e-gov) modernisation, and to some extent, to the new norm due to the COVID-19 pandemic.

Typically, citizens have high expectations when interacting with e-gov services, since they are used to highly efficient and promptly delivered solutions already provided by businesses in their everyday lives. This can be observed, for example, for smart homes, e-banking, electronic restaurant kiosks, smart vehicles, and airports. A constant expectation from citizens is that e-gov services will keep the same pace of efficiency, and that e-services in general will swiftly adapt to their needs, which in part is realised by collecting and sharing information. In the EU, this expectation goes even further since e-services should also consider the cross-border nature and mobility of citizens across multiple countries. For instance, prominent examples of such services are the Schengen Information System (SIS) and the Customs Decisions System (CDS). The former is the most widely used and largest information sharing system for security and border management in Europe, while the latter comprises a central system to be used for all applications and decisions which may have an impact in more than one Member State (MS).

EUIBAs are dealing, more and more frequently with sensitive information. In many cases such information is not classified, but it is, nevertheless, sensitive, for its impact in term of privacy, data protection, or for its potential policy and political implications. On top of this information some of the EUIBAs deal also with classified information. The increasing digitalisation and the effects of teleworking due to the pandemic, are making in general more difficult, or too cumbersome, the application of the different measures concerning the higher level of restriction, both within each institution, and in the case of inter-institution information exchange.

EUIBAs rely on a growing variety of IT infrastructures and services to fulfil their role, from low-level networking functionality up to advanced collaborative apps and tools relying on secure information storage and sharing. Without being exhaustive, the following list includes a few types and instances of IT services (assets) that are commonly necessary within the EU entities:

- Low level connectivity and networking services including internet/intranet connections, domain name services, proxy and internet address filtering, and so on.
- High-level online services including search engines, web browsing, and translation.
- Remote access to IT infrastructures including virtual private networks and remote desktop services.
- IT service and system management including operating system management.
- Information security and data protection services, including host-based intrusion detection systems, identity management (EU Login), public-key infrastructures for secure information exchange, web presence protection, cybersecurity management tools, antivirus, etc.
- Productivity apps including e-mail, contacts, and calendar service, say, MS Outlook.
- Business apps including project management, survey tools, and others.
- Collaborative environments including instant messaging, videoconferencing, say, MS Teams, meeting organisation services, file sharing, e.g., Owncloud, instant pools, say, Slido pools, to mention just a few.
- Digital services provided to MSs, for example those concerning VAT and Excise systems, those used for border management (Entry Exit System, ETIAS, SIS, VIS), those concerning the nuclear safeguards treaties, and many more.

The key factor, under the perspective of this report, is that all these services are daily used to treat and exchange, different types of information which are for one or another reason impactful for the life of the Union. Financial information, draft legislations, results of analysis and monitoring activities, but also information related to investigations, security and defense documents and strategies, in short, politically sensitive information which, if not handled correctly, might have a negative impact on European citizens, countries and industries. On top of this is important to note that most of the digital technologies used to implement the digital services used for the mentioned operations are provided by non-European (mainly US) countries, and that the majority of the utilised hardware is also produced outside Europe. This not only poses the well debated question concerning strategic autonomy of Europe concerning digital services, but also a question on the level of trust Europe should have on these products and services when coming to the handling of potentially sensitive information.

Due to the high number and diversity of IT services and sometimes the lack of in-house expertise, EUIBAs heavily rely on outsourcing of their IT infrastructure and on external ICT service providers and contractors. Furthermore, specific EU entities manage government services that have special business requirements related, say, to border security and cybercrime, as for example Frontex and Europol. In such a case, the high confidentiality and criticality of the information handled and processed, renders risk assessment imperative as well as a clear set of rules for the handling of information.

Classified information may be exchanged with MSs, which have defined equivalent national levels of information of classification[5] In this case, a critical point is to maintain an up-to-date registry of information security tools, such as cryptographic products that have being assessed and certified to be used to exchange in secure way this type of information not only within EU institutions, but also across MSs. This registry of tools is of key importance to ensure that collaboration and exchange of sensitive information is trusted among EU organisations and national authorities, since the lack of trust may be a hindering factor regarding information sharing intentions. The adoption of a commonly recognised and accepted registry would also facilitate the speed-up of the agreement process among institutions when classified information needs to be shared.

Cloud migrated services and virtualisation in general are another key factor that calls for revisions regarding the information risk assessment process. Precisely, regarding the adoption of cloud-based solutions, numerous new concerns arise related to the storage, communication, and processing of information. Concerning the adoption of such solutions, information with a limited need-to-know may be inadvertently or otherwise exposed due to the sharing of cloud infrastructures with other

[5] COMMISSION DECISION (EU, Euratom) 2015/444, Annex I

enterprises. Also, the provider's authorised personnel, and potentially powerful third parties, may have access to such data.

Standard approaches to mitigate the exposure of this information stored in outsourced cloud services is the use of overlay encryption, such as, MS Double Key Encryption, or, if possible, the adoption of an interoperable hybrid cloud approach partially outsourced, where information with a limited need-to-know does not leave the organisation premises. Furthermore, depending on the type of the adopted cloud solution, e.g., infrastructure, platform, or software-as-a-service, vendor lock-in becomes an important threat to the availability of the information. Finally, cloud-based solutions provided by non-EU countries face the additional boundary of legal disclosure of EU information with a limited need-to-know by national security or law enforcement authorities of these countries.

To cover a plethora of use-cases, including online collaboration, document management, and conference services, the current situation is rapidly moving towards the large-scale adoption of cloud-based software-as-a-service (SaaS) solutions, such as MS Office 365. While such swiss-army-knife and one-size-fits-all solutions seem efficient, they may still exhibit security weaknesses similar to any relatively new software product. The OWASP security by design principle titled "don't trust services", i.e., external systems must not be trusted, is self-explanatory to this point. The key point here is a serious reflection on the dependency of Europe on Third country (mainly US) software and third country (mainly Asiatic) hardware, which in the long term might have the potential to amper the autonomy and the secure handling of European sensitive information.

Excluding legacy weaknesses and vulnerabilities, the adoption of a SaaS hosted by non-EU cloud providers has a large potential for exposing information with a limited need-to-know to third country law enforcement authorities and requires strict countermeasures. For example, using SaaS solutions to store and manage sensitive non-classified (SNC) information requires a homogenous and aligned approach for encrypting this information in an end-to-end manner.

Outsourcing in EUIBAs may also involve the subcontracting of information security tasks, including the development and management of information systems handling data with a limited need-to-know. Moreover, sensitive functions may include risk assessments, drafting of security plans, logging and analysis of information security events, and the detection and forensic investigation of cyberattacks.

Overall, as already underlined, the issue of "trust", reflected to an increased risk, does not only pertain to outsourced and cloud-based systems – it is pervasive. Namely, from a European viewpoint, nowadays, a critical mass of major technology stems from the US and runs on hardware that is produced in China. This may require some sort of vetting on these technologies/products before entering the European market. For instance, before a piece of software is imported and sold in EU, its source code can be examined to ensure that is, e.g., rootkit-free. This issue is tightly related to the supply-chain threat discussed in section 2.2.2.

2.1.3 The "new norm" due to COVID-19 pandemic

The so-called new norm, currently adopted worldwide due to the COVID-19 pandemic, makes teleworking the default choice across many sectors, naturally affecting EU entities as well. Nevertheless, the reality quickly demonstrated that the massive adoption of teleworking goes hand in hand with new complicated information security challenges, since among others, information with a limited need-to-know is now exchanged to/from home networks, sometimes with the use personal devices. And the COVID-19 "pile-on effect" found many EU bodies unprepared to face urgent teleworking security challenges.

One could say that COVID-19 has abruptly thrown security into the public awareness; threat actors are suddenly offered a lot of new surfaces to attack, and each teleworker is now a bit more accountable than they were for their organisation's information security.

As a matter of fact, this pandemic-spurred "cyber insecurity" has been repeatedly pinpointed by major surveys, which also call for re-consideration of relevant strategies, policies, and risk management plans.

A recent report titled "Enduring from Home: COVID-19's Impact on Business Security" [13] released by Malwarebytes points out that since the start of the pandemic, teleworking has been the cardinal reason for security breaches in 20% of organisations. Also, 24% of the survey respondents, mostly IT and cybersecurity professionals, said that their organisations had to pay unexpected costs to address cybersecurity breaches or malware infections after teleworking was deemed necessary. Even more, 18% of participants claimed that cybersecurity was not a priority, and 5% admitted that their staff were "oblivious" to best security practices. The report stresses out that organisation email compromise, the rapid shift to cloud services, and the insufficiently configured and secured Virtual Private Networks (VPNs) are the three major contributing factors to this issue. Another point, confirming the already gloomy picture, is that phishing email rates relating to COVID-19 have soared. As a characteristic example, the UK National Health Service's key workers were bombarded with roughly 40,000 spam and phishing attempts between March and the first half of July 2020. On top of everything else, 45% of the participants said that no extra security audits were done to assess the security posture of these unavoidable changes. And while 61% of organisations did equip their staff with remote working devices, 65% neglected the deployment of new security tools to support this equipment.

The 2020 data breach report published by Verizon [14] concludes that due to teleworking, security vulnerabilities have surged. That is, credential theft, errors, and social attacks comprise the triad of most common causes that lead to a breach, and teleworkers may be particularly vulnerable to these attacks. According to the report, the reliance on remote workers is also tightly associated with the emergence of brand new cyberattack tactics. The report ends up to several interesting observations.

- 72% of breaches involved large business victims.
- 58% of victims had personal data compromised.
- 70% attacked by external actors, but espionage accounts for just 10% of breaches in 2020.
- Organised criminal groups were behind 55% of breaches, while 30% involved internal actors.
- 45% of breaches featured hacking, 22% social attacks, and 17% malware.
- 8% of breaches were misuse by authorized users.
- 86% of breaches were financially motivated.
- 67% of breaches are due to credential theft, social attacks, that is, phishing, business email compromise, and errors.
- Ransomware accounts for 27% of malware incidents.
- Attacks on web apps were a part of 43% of breaches; this figure has been doubled from that of 2019. Naturally, as workflows migrate to cloud services so do the attackers.

Especially for public administration services, the same report concludes that "ransomware is a problem for this sector, with financially motivated attackers utilizing it to target a wide array of government entities. Misdelivery and misconfiguration errors also persist in this sector".

The report also provides the following interesting figures specifically for the public administration sector:

- Frequency: Almost 7K incidents, 346 with confirmed data disclosure.

- Top attack patterns: Miscellaneous errors, web apps, and everything else account for 73% of breaches.
- Threat actors: External (59%), internal (43%), multiple (2%), partner (1%).
- Actor motives: Financial (75%), espionage (19%), fun (3%).
- Data compromised: Personal (51%), other (34%), credentials (33%), internal (14%).
- Top controls: Implementation of a security awareness and training program, apply stricter boundary defense, secure configurations.

Another 2020 report by Kaspersky [15] verifies that the rapid shift to teleworking has taken corporate security by surprise. Indeed, in most cases, risk assessment has not been promptly or even at all re-evaluated to adjust to the "new normal" at the "redefined workplace". . On the other hand, cybercriminals quickly adapt to new opportunities for compromise. For instance, there is a high increase in COVID-themed phishing attacks, where impostors pretend to be healthcare organisations. The report pinpoints that, now, hackers take advantage of the fact that on the one hand remote workers use corporate equipment for personal tasks and on the other, they use corporate networks via unsecured or inadequately secured personal devices. Moreover, the way teleworkers connect to the corporate network is vital. As a matter of fact, the report states that from March 2020, there is an acute increase in attacks on network ports open for Microsoft's remote desktop (RDP) app.

In absence of face-to-face contact, teleworkers exploit other ways to collaborate. It is for sure that some of them employ software tools not endorsed by the organisation, say, because they find these tools easy to install and use. For example, as stressed in the report, "a Google Docs document with certain access permission configurations may be indexed by a search engine, leaking corporate data". Moreover, it is not to be forgotten that the Zoom videoconferencing platform has been recently criticized for potentially sharing user data with Facebook, without asking for the user's permission. Recently, FBI has also emphasized on the fact that a range of threat actors have been hijacking videoconferencing apps, including Zoom and Microsoft Teams [16]. The same major worry applies to data stored in the cloud. For instance, a by mistake or randomly added outsider in a collaboration tool could be granted access to the full hierarchy of files and messages. No less important, not every employee has access to corporate equipment, say, laptops, so some of them are inevitably use their home computers. This however poses a serious threat for organisations lacking a well-defined Bring Your Own Device (BYOD) policy. And on top of everything else, teleworking should be an integral part of a cultural shift to digital transformation, which at least for the moment is in prospect.

2.1.4 Shared challenges

Shared challenges for EU organisations can be organised in the following axes.

1. Individual challenges that are common to most of EUIBAs and could be addressed more efficiently if a joint set of information security rules is established.
2. Challenges that emerge due to the need of collaboration and sharing of information with a limited need-to-know among EU organisations.

Specifically, every EUIBA is expected to adhere to a high standard of information security, which is difficult to establish considering the variety of the sizes and available resources of these organisations. Under this prism, few would object that the biggest benefit of the definition and adoption of common information security rules by EU organisations is the possibility of a shared effort with respect to the implementation of these rules. Among others, this could include the definition of standards for selection and assessment of trusted cloud providers, development of interoperable information exchange formats, e.g., publications office taxonomies, collaborative assessment of threat and risk models for common scenarios, and others. Notably, the sharing of efforts is particularly beneficial for small EU organisations that have limited resources and in-house

expertise to be effective with respect to the implementation and operationalisation of their information security processes.

As an indicative example of the diversity that may exist in security practices followed by different EUIBAs, we refer to the preliminary results of a fresh study[6] examining the level of adoption of modern security standards in email communications by EU organisations. As shown in Figure 3, the results of this study clearly suggest that not only there is a significant gap in the adoption of contemporary e-mail security standards designed to protect e-mail communications, but also there exist notable disparities among the approximately 60 different EU network domains tested.

Simply put, no universal policy applies, meaning that each institution or agency adopts a subset of these standards depending on the case and the available expertise.

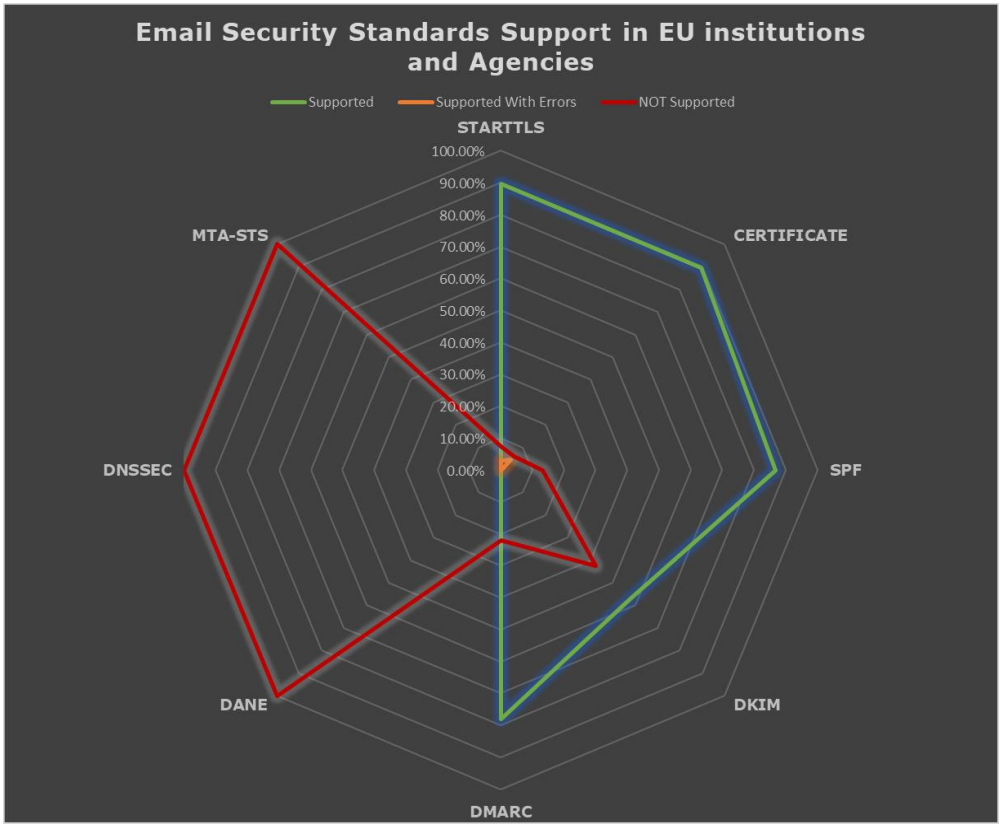

Figure 3. Percentage of EUIBAs supporting different email communications security standards.

EU organisations are also expected to establish and maintain a network for coordination of information threat intelligence information, including threat reports and near real-time collaborative information security breach response. With reference to the previous subsection, considering the outsourcing of sensitive functions, contractors delegated by EU organisations should collaborate on behalf of the EU organisations in this respect. To enable this information sharing, a common approach and language/terminology is of fundamental importance.

Considering the sharing of information with a limited need-to-know, EU organisations could benefit from a universally applied information management scheme, including common classification labelling criteria and common metadata classification (to univocally identify data types and classes). Such a strategic approach could enable the deployment of an interoperable Data Loss Prevention (DLP) solution to detect and prevent data breaches by data exfiltration in a seamless way. This

[6] The study has been performed by means of the mecsa-st command line, a tool developed by JRC to assess the support of email communications security standards. The tool is publicly available at: https://github.com/mecsa/mecsa-st. The authors of the report would like to thanks Ignacio Sanchez and Gerard Draper from JRC.E3 unit for having provided the data showed in Figure 3

ambitious objective can only be achieved adopting a common high standard of information security protection, a common set of processes and techniques and a common set of classification and labelling systems, all supported by a tight security information sharing approach across all the European institutions. EU organisations would be in position to securely exchange SNC or even EUCI in digital format. On top of that, by adopting a common set of information security rules, end-user security awareness programs and training can also be collaboratively established, leading to higher efficiency and reduced investments. Reuse can take place in multiple realms to avoid duplication of efforts and conserve costs. An example of a common methodology already taking place is the so-called IT Security Risk Management Methodology (ITSRM^2) developed by DIGIT. This methodology is in line with Commission Decision 2017/46 on the security of communication and information systems (CIS) in the European Commission.

2.2 Risk identification

Generally, there exist several rudimentary factors that can be used to characterise or identify a risk.

- Its **origin** referring to one or more threat agents, i.e., an individual or group that can manifest a threat, including dissatisfied, terminated or poorly trained employees, hackers, competitors, state-sponsored agents, chaotic actors, espionage, cyberterrorists, etc.
- A given **incident** pertaining to a threat. That is, a sudden blackout, unauthorised access to confidential data, a privacy violation, the introduction of new regulations regarding security and privacy policies, the migration of some processes to a new system or to the cloud, the outsourcing of a given activity or service, etc.
- Its **consequences or impact**, including service outage, economic damage, loss of reputation, prestige and competitiveness, financial penalties, etc.
- A **specific reason** for its happening assigned to a set of vulnerabilities. That is, poorly designed and tested software, faulty or deficiently maintained hardware, unprotected storage, lack of audit trail, complex user interface, problematic password management, etc.
- The **existing defensive schemes and controls**, including thorough background checks on critical staff, the implementation of baseline and detailed security policies, role-based access, intrusion detection and prevention systems, security training and education, participation to cyber-intelligence programs, etc.
- The **time, circumstances, and place of occurrence**; think for example of extreme weather conditions, earthquakes, terrorist attack anniversaries, demonstrations and strikes, a fire, etc.

Also, pertinent questions to this regard are:

- What assets are of interest?
- What threats should we look for on our assets and why?
- Why might our information be attacked and by whom?
- What activity are we seeing?
- Where has this threat or attack been seen before?
- What does it do?
- What vulnerabilities does this threat exploit?
- Why does it do this?
- How can these attacks be implemented?
- Does the information security incident encompass misdirection or misleading information injected by the opponent?
- Is this threat persistent?
- Is this threat related to or affects others?
- Who is responsible for this threat?

Having the above questions in mind, risk identification is split into five steps, namely identification of assets, threats, existing controls, vulnerabilities, and consequences.

2.2.1 Assets

Assets can be categorized either as primary or supporting. The former includes the organisation's activities and processes and all sort of strategic, vital, personal, and high-cost information which is collected, kept, and managed by the organisation. The latter include assets on which the primary assets rely for completing their mission, namely hardware, software, networking infrastructure, personnel, site, and so on. The supporting assets are potentially prone to vulnerabilities exploited by threats, and in such a case, the harm is reflected on the corresponding primary assets.

Recall from section 0 that, in our case, the assets of interest are any type of information, either classified or non-classified with a limited need to know, and thus they belong to the primary category. A coarse-grained categorisation of these assets is given in Table 1.

Table 1. High-level, non-exhaustive categorisation of information assets. The "C" character denotes a possibly critical asset.

Category	**Description**
Facilities management information	General infrastructure Security infrastructure (C)
Financial management information	General finance information Management information regarding budget and report
Governance, diplomacy, strategy, and committees management data	Member States data, e.g., information exchanged with MSs public administrations and National Competent Authorities, National inquiries, National Classified Information originating from MSs, etc. (C) Defense-related data, e.g., procurement, military support activities, intelligence, European anti-fraud office investigations, classified, etc. (C) International diplomacy and foreign relations data (C) Court procedural documents (C) Opinion of the Legal Service documents Policy information Legislative documents Strategy documents (C) Working documents (C) Audit and risk management, including Internal Audit information Meetings schedules
IT support information	Communication and collaboration (C) Information (C) Infrastructure information Identity and access information (C) Technology procurement information

	Technology support information Log files (C)
Human resources information	Staff and employee records and personal identifiable information (PII), including retirees, trainees, and external collaborators Recruitment information Records of health, safety, and environment (C)
Media	Websites Social media information
Research information	Research management data Research results (C) Publications Contract management Intellectual property
Learning information	Online learning information Course information Library learning resources Metadata
Information from third parties	Information seized during investigations (C) Defence information (C) Industrial information, e.g., for chemicals regulation, nuclear regulation Information received from outside-EU cooperation partners, e.g., for EUROPOL (C) Classified Information coming from third Countries and International Organisations, etc. (C)

2.2.2 Threats

Threats are not static, but constantly evolving becoming more sophisticated, and may affect one or multiple assets, causing diverse impacts on each of them. Harm can be due to a human or not, e.g., think of a cybercriminal versus a flood, and can be deliberate or by oversight. On top of conventional threats, today, globalisation, facilitated by rapid technological change and global interconnectivity, has given a dramatic impetus to the phenomenon of hybrid threats.

For the needs of this report, and as explained further down and in Figure 4, we rely on an attacker centric threat model. Such a model starts with the attacker and evaluates their goals and the ways they might accomplish them. The level of adversarial misbehaviour is considered as well. That is, the analysis separates between malicious and semi-honest (also known as honest but curious) parties and between insiders and outsiders. A semi-honest party abides by the security policy, say, regarding the provision of a communication service, with the exception that they will keep a record of all the

received messages and transactions, and will try to manipulate the recorded messages in an aggressively adversarial manner to learn additional information. A malicious party on the other hand can misbehave in arbitrarily ways, i.e., they may terminate the communication protocol or procedure at any stage or change, manipulate an input before entering the protocol, or even destroy assets.

A particular interesting case of threats, which may be a greater concern today pertains to what it is called the "insider threat", i.e., individuals with legitimate access to an organisation's assets. This threat is often overlooked and not proactively dealt with by organisations. Generally, one can discern between three major types of human insider:

- Those who willingly try to inflict damage to their organisation, say, via theft of intellectual property, espionage, fraud, sabotage, etc.
- Non-malicious insiders who may consciously infringe the organisation's security policy, but they do believe that this will benefit their organisation; For instance, in many cases, employees bypass security policies or come up with shortcuts in sake of improving their job.
- Unwitting insiders who are not even aware that they are acting wrongfully. This type of insiders is considered especially hazardous to organisations, as they are highly prone to social-engineering attacks exfiltrating information, and malware. Recall that the compromise of human assets is in many cases the premier step in a security incident, even if the rest of the systems are safe.

As the world becomes increasingly interconnected, another emerging source of threats pertain to the lack of robust processes to identify and manage the growing supply-chain risk. Nowadays, even sensitive products, including defense ones, embed electronic components, e.g., circuit boards, which may stem from regions where the original equipment manufacturer is not even aware they have a supply chain. This leaves room for supply chain attacks targeting the most feebly secured elements in the supply chain, where, typically, the attacker tampers with the manufacturing process of a product by installing a backdoor, rootkit, or hardware-based spying components. Simply put, organisations increasingly rely on third-party ways to establish supply-chain trust, and to our knowledge there is no concrete national or international legal/regulatory way to address this issue. And naturally the problem is aggravated with enterprises becoming gradually more reliant on third-party suppliers. A globally agreed chain of trust based on e.g., blockchain or public key infrastructure (PKI) may offer a solution to this problem, but this remains a long shot at the moment.

All in all, threat identification should especially consider threats originated by humans either insiders or outsiders. Precisely, there exist multiple ill-motivated groups that may weaponise threats, including script-kiddies, hackers, cyberterrorists, hacktivists, cyberespionage groups, foreign governments, intelligence and counter-intelligence agencies, cybercriminals, and so on. Amongst others, threat identification and analysis stemming from such groups should be done vis-à-vis the group's motivation or objectives, including monetary, revenge, political gain, political or other sort of activism, fraud and e-crime, theft of intellectual property, espionage, rebellion, greed and opportunism, religion, desire or obsession, anger, ego, self-promotion, curiosity or boredom, convenience, worldview, unintentional and by oversight errors, etc. It is not to be neglected that attackers of any kind need method, opportunity, and motive. At minimum, the output of this phase should be the list of the identified threats along with their type and origin.

As mentioned in section 1, for the current phase and for the threat analysis part, a slightly modified version of the "Security cards" threat brainstorming toolkit was exploited. This toolkit focuses on four dimensions, namely:

1. Human impact - for the needs of this study, the human impact has been adjusted to represent the organisation impact dimension.
2. Adversary's motivations.
3. Adversary's resources.
4. Adversary's methods.

Organisation impact: Concentrates on the various ways in which the organisation or associated third parties can be affected if data with a limited need-to-know are leaked, altered, made temporarily

unavailable, or destroyed. In the event of such an incident, the following angles of thought are of interest.

1. It may inflict **economic** damage and harm the **reputation** of the affected parties. The damage may be confined to one party, say, an agency or, due to the ripple effect, spread across many parties, including MSs and other EU institutions. Leaked data may be exploited in nefarious ways to polarize the public opinion, alter public discourse, and/or cause fear, anger, mass hysteria, or confusion to the public.
2. If **personal data** are leaked, say, personnel medical records, browsing history, email content, etc., it may facilitate identity theft, blackmail, extortion, and slander, among others. Excluding regulatory penalties and any other sort of direct or collateral damage to the organisation, this may also have direct or indirect impact on certain people's physical wellbeing.
3. A direct or indirect impact may be perceived on **relationships**, either inter-organisational, international, or inter-personal in some cases. This also leads to loss of reputation.
4. Leaked data may reveal **information** about critical infrastructures and cyber-physical systems in general. Therefore, if these pieces of information are exploited maliciously, it may have a direct or indirect impact on critical services or the biosphere, say, inflict power outages, pollute water sources, cause fires, paralyse data centers, expose government or military secrets, etc. As already mentioned before, the Commission, per se, manages directly very few critical infrastructures (e.g., the nuclear facilities and critical laboratories operated by the Joint Research Centre), moreover few agencies or EU Bodies operate directly critical infrastructures (e.g., few installations of ESA, the Galileo system etc.). But this is only a small portion of the information on critical infrastructures handled by EU bodies. In fact, due to their role of secretariat and coordination of cross-border initiatives among MSs, due to monitoring roles (e.g., nuclear safeguards, EMA etc), or to liaison duties (e.g., participation to NATO meetings etc.) EU bodies and institutions are recipients of many sensitive information concerning critical infrastructures.

Adversary's motivations. It focuses on the reasons an individual or group might wish to assault the information system. Here, the adversary may use or abuse the information system:

1. Because it is more convenient in comparison to other alternatives or because it is the sole way to achieve their purposes. This motivation applies to both insider and outsider types of threat actors. For instance, an insider may bypass the organisaton's firewall or attempt to connect to a protected wireless network with the aim of gaining access to shady webpages, which in turn may drop malware to their PC. Then, the malware could exfiltrate classified information in a persistent manner. Any system with restricted permissions is potentially vulnerable to this threat.
2. To satisfy curiosity or to ease boredom. This also concerns both insider and outsider types of threat actors. The more alluring the protected information, the higher the possibility for such a threat to materialise. An unlocked door, an easy-to-guess or crack Wi-Fi password may give the opportunity to the attacker to infiltrate to restricted areas, e.g., an administrator or secured area, where information with a limited need-to-know is stored.
3. To satisfy a desire or obsession. For instance, the opponent, either insider or outsider, may need specific protected information for exercising sexual or other kind of blackmail. They may also exploit covert webcams and wearable tech or passively monitor communications for obtaining the information of interest.
4. To obtain an advantage in diplomacy or warfare (one of the most likely scenario for what concerns EU bodies). This threat pertains to state-sponsored actors and other types of powerful in terms of skilfulness and resources adversaries. Information regarding critical infrastructures, emergency systems, defence systems, medical research records, or other type of high-stake information are the typical targets of such an opponent. Their goals may range from gathering data to spreading misinformation, disable equipment, cause distractions, and paralyse communications.

5. For evil intent or revenge. This applies to both insider and outsider kinds of threat actors. Think of a dissatisfied or discharged employee, a compelling antagonist, etc.
6. For financial gain. The goals here are clear; sell the acquired information to the highest bidder, extort the organisation, sabotage the system, manipulate information and relevant decisions, and so on.
7. To affect politics. This case typically involves strong threat actors. The adversary's aim may be to discredit political figures, polarize public opinion, cause anger, change the public's understanding about a matter of debate, etc.
8. For self-protection or to protect third parties. This mostly applies to insiders. For instance, an employee may decide to cover up a data exfiltration incident with the purpose of protecting a colleague with whom they are having a sexual relationship.
9. To promote an ideological stance, or a religious, political, or other kind of agenda. This motivation pertains to both insider and outsider types of threat actors. Keywords here are hacktivism, environmentalism, animal rights, drugs, sexuality, and more.
10. For self-promotion or to gain fame. An outsider may attempt to hack into challenging systems, deface a well-protected website, crack an encryption scheme, and so on just to prove their skilfulness and for gaining notoriety. And, naturally, EUIBAs are a very alluring target to fulfil this goal.

Adversary's resources: It refers to the different assets an adversary may possess, including money, dexterity, software and hardware tools, and their capacity to influence the actions of others or collide with groups of people. We particularly concentrate on the following aspects:

1. The levels of expertise the adversary already has or can potentially obtain. From a low to higher level of expertise, one can differentiate between script-kiddies, hobbyists, security professionals, including all kinds of hackers, proficient con artists, and state-sponsored actors. More specifically, we consider the following categories.
    a. Non-tech-savvy: They have access to certain areas of the information system and may be interested in specific pieces of data that possibly are communicated in the clear or leak due to the inexpediency of some protection measure. Such opponents are basically semi-honest, behaving according to the protocol, but interested in learning as much information as possible.
    b. Advanced: They have the knowledge, technical skills, and considerable resources to exercise any attack against the information system. Their goals include DoS or causing commotion, monitor all kinds of network traffic, etc. This category embraces any kind of hacker, researcher, security professional, etc. These actors are supposed to be mostly malicious, but in certain cases, they can also be honest-but-curious, e.g., academic researchers.
    c. Powerful: They comprise advanced adversaries with unlimited resources, hence, they are in position to exercise any kind of attack, including persistent ones, in large scale, say, conduct tactical espionage operations or infiltrate and obtain complete control over the system's infrastructure. Amongst others, they typically seek to learn information and extrapolate conclusions about the system's inner workings, sabotage, cripple, or paralyse the system, inject bogus notifications that would cause panic, undermine the credibility of the system, and subvert the authorities. This category encompasses state-sponsored actors and large organisations
    d. Peripheral: If motivated properly, say, monetary gain, bribe, revenge, corruption, extortion, and hacktivism, these insiders might act individually or, more likely, collude with others, either outsiders or insiders to inflict damage or exfiltrate confidential information. This category includes members of the family, system administrators, and persons working in key positions in other EUIBAs, and thus, their capacity depends on their role in the organisation. For example, they may have admin access or possess a special badge, granting them privileged access and elevated power. Such actors are mainly classified as honest-but-curious with more legitimate information available,

but malicious behaviour is not to be ruled out, e.g., think of a dissatisfied employee and a paid-off official.

2. Opportunities that might be available to the adversary in the future. For instance, anticipated changes to the underlying IT infrastructure or technology, say, a migration of some service to the cloud, direct or indirect access to a product along its supply chain, sudden and incompatible rise in teleworking and digital workplace due to the pandemic, etc. In fact, increased connectivity and reliance to external parties may significantly augment the attack surface, creating room for new targets and stealthier, low-cost, and more effective assaults.
3. The adversary's level of confidence they will remain anonymous, and thus they will go unpunished. Impunity for their actions may make adversaries bolder to mount more persistent attacks against the system. Think for instance of government sponsorship, employment of network anonymity tools like Tor and I2P, diverse legal and judicial systems, e.g., a cloud service that is subject to US law, etc.
4. Inside capabilities, knowledge, and potential of collusion. Physical access, user versus admin account, system backdoors, a collaborating insider, blackmail, bribery, installation of rogue hardware, ability to forge official documents, knowledge about system usage, maintenance patterns and implementation details, knowledge about bureaucratic processes, access to former or retired employees, capability to access discarded documents, say, via dumpster diving, and so on are factors that are relevant to this respect.
5. Access to liquid assets, i.e., those that can be easily converted into cash in a short amount of time. For instance, organised crime, corporate, or state-sponsored adversaries are in position to purchase equipment, pay bribes, and hire expert help.
6. Adversary's level of power or influence. A powerful adversary may be in position to affect laws or regulations, coerce employees, influence co-workers, establish covert groups, etc.
7. Timeframes or conditions: How different timeframes may enable the adversary to mount attacks? For instance, if cryptographic keys are not ephemeral, then the assailant has more time to try to break encryption. A special condition, say, a scheduled system maintenance may provide more opportunities for them to exercise an attack.
8. Specialized hardware, software, or other equipment. One can mention sophisticated cryptographic key/password crackers, reverse-engineering tools, rogue access points, stingrays, etc. Naturally, the amount, quality, and strength of these tools directly depend on the adversary's profile. For instance, a state-sponsored adversary may have access to unrestricted resources.

Adversary's methods: It examines the general ways an adversary might attempt to attack the information system. Methods can range from a legacy technological assault, to manipulating (though social engineering), bullying, or coercing specific persons, camouflaging or wiping out evidence and causing distraction, and leveraging bureaucratic and human nature within the system.

1. Attack footprint: The adversary typically attempts to conceal, diminish, or eliminate the evidence of their attack and possibly incriminate another party. To this end, they may try to wipe out hard drives, delete or manipulate log files, anonymise their identity and location, use a reflector, attack in a low-and-slow manner, inject bogus attack traces, use an attack-as-a-service provider, etc.
2. Unforeseen or neglected properties of the system: The adversary may take advantage of indistinct or not straightforward to anticipate system characteristics to infiltrate into or exfiltrate data from the system. For instance, a side-channel type of attack, or a misconfiguration in the operating system may allow them to retrieve a Wi-Fi key.
3. People manipulation: Impersonation, phishing, water-holing, blackmailing, bribery, and a long range of social-engineering techniques can be very profitable for, say, dropping malware, obtaining physical access, destroying or manipulating audit logs, convincing people into divulging information or performing actions that have an adverse effect on the confidentiality or integrity of the data.

4. Multi-stage or multi-layer attacks: The attacker starts with a simple attack on a certain (low) layer and escalates it to higher ones. Say, they exercise a DoS attack on the corporate Wi-Fi, while at the same time install a rogue access point with the aim to exercise a captive portal attack and steal Wi-Fi passwords. Then, they gain foothold on the network, enabling them to persistently exfiltrate data.
5. Physical access: An adversary with physical access to the system can install rogue hardware or software, eavesdrop on possibly unencrypted intranet communications, tamper with hardware to deactivate security controls, inject false alarms and create commotion to misguide the IT security team, install keyloggers, destroy equipment, access confidential files, and so on.
6. Technical and bureaucratic processes: The adversary may take advantage of certain processes, including backups, password recovery, error recovery, scheduled system maintenance, helpdesk, etc.
7. Tech attacks: A vast range of passive or active attacks fall into this category, including eavesdropping, DoS, spoofing, replay, and malware including ransomware.

Based on the above discussion, a basic threat model is given in Table 2. Note that the analysis on the properties of each threat is indicative, and thus non-exhaustive.

Table 2. High-level threat model focusing on key threats

Threat	**Motivation**	**Intention**	**Threat events**
Cybercrime	Financial	Unauthorized access, deny access, infrastructure hijack	Malware, hacking, social engineering, abuse, botnets, stolen credentials, fraud.
State-sponsored espionage	Intelligence, political, diplomacy, warfare, realisation of a hybrid threat.	Unauthorized access, Data gathering, creating destabilisation, polarisation, chaos, panic, frustration, sabotage.	Social engineering, tailored malware, persistent access and exfiltration of data, credential harvesting, collusion with other parties, including a cloud provider. Multi-stage, multi-layer attacks.
Human errors	Carelessness	N/A	Eavesdropping on unprotected or unattended information, loss of (portable) devices or storage media, unattended office or building, BYOD policies, careless behavior when

			interacting with social media.
Opportunists	Egoism, fun, self-assertion, curiosity, boredom, desire, obsession, revenge, self-protection, opportunity to exploit the weakest link.	Exploitation, Infrastructure hijack	Hacking, DoS.
Hacktivists	Ideology, political, religious.	Damage of reputation, sabotage	DoS, spear-phishing, watering-hole attack, website hacking.

2.2.3 Existing controls and legislation

EUIBAs already implement controls defined by a set of security policies, standards, guidelines, and technical specifications. Besides, this is governed by the relevant legislation. For the European Commission the foundation of these controls is in Commission Decision 2015/443[7] on security in the COM and Commission Decision 2015/444[8] on the security rules for protecting EUCI as well as in Commission Decision 46/2017[9] on the security of the communication and information systems in the COM. Security policies, standards, guidelines, and technical specifications are provided for many specific areas including technical standards. The following list summarises the current information security related elements already addressed by Commission institutions:

- Access control and authentication.
- Accreditation process for communication and Information systems handling EU classified information.
- Backups.
- Business continuity management.
- IT Security Compliance.
- Controls against malicious code.
- Symmetric and asymmetric cryptography
- Information security risk management
    - IT Security Risk Management Methodology.
    - IT Security Plan.
    - IT security risk management – Mapping levels for Confidentially, Integrity and Availability.
- Information systems security incident management.
    - Security incident management and incident notification.
- IT asset management.
    - ITSRM^2 Business impact level scale to IT asset priority label mapping.
- IT vulnerability and remediation management.
- Logging and Monitoring.
- Mobile code.
- Operational management.
- Outsourcing of communication and information systems.
- Passwords.

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D0443
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D0444
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1484304449216&uri=CELEX:32017D0046

- Physical and Environmental security.
- Powershell.
- Removable media.
- Sanitisation of media.
- Secure systems development.
    - Secure systems lifecycle – S^2LC.
- Transport Layer Security (TLS).
- Web application security standard.
    - Web application secure development guidelines.

More in details, here below we present key points which are inspiration of discussion from different pertinent EU Documents:

C(2019) 1904 final, Security Notice Marking and handling of sensitive non-classified information addresses many elements concerning the handling of sensitive-non-classified information. It states that:

Concerning sensitive information:

- Electronic copies should be stored on platforms that can only be accessed by the target audience. The use of encryption and digital signatures is recommended, taking into account the risks and other countermeasures in place.
- Scanned copies of documents, including both electronic and hard copies, should be removed from any insufficiently secured locations as soon as possible, including shared drives, unencrypted emails, scanner device memory and printers in unsecured office areas.
- Where email is used to transmit SNC information, even partially, the use of the Secure email (SECEM) application (or similar) is mandatory, i.e., the emails must be signed and encrypted.

Concerning special handling:

- Electronic copies should be stored on platforms that can only be accessed by the target audience. The use of encryption and digital signatures should be considered, taking into account the risks and other countermeasures in place.
- The originator may direct that documents must not be stored in document handling systems but only the metadata (document title, originator, reference number, etc) may be registered there. The metadata, including the document title, should not reveal SNC information.
- It is important to notice here how indications are given about procedure to follow, but nothing is provided for what concerns the techniques, tools mechanisms to put in place, except for the use of SECEM or similar. The “mention” to the use of SECEM or “similar”, indeed magnifies a notable issue in the handling of sensitive (or even classified) information, especially in the context of sharing outside EC institutions, i.e., the clear establishment of an equivalence between security controls, tools, and measures. To remain on the example of SECEM, the question, in case of information exchange with institutions not provided with SECEM is “what is equivalent to SECEM”? What the other institution can use? Which are the requirements of the tool to be used for such cross-institution exchanges?

COMMISSION DECISION (EU, Euratom) 2017/46, on the security of communication and information systems in the European Commission, does not either cover this particular aspect. In fact, it defines at high level roles and duties concerning the management of communication and information systems security. However, best-practices, guidelines and standards are not mentioned. DIGIT is tasked, in collaboration with HR-DS to identify, implement and monitor these procedures. This obviously applies only to the Commission, hence other EU bodies for the same type of systems might have different procedures and controls, leaving open the question regarding equivalent security measures to be used to share (and store) information.

Commission Decision 2015-444-EUCI, clarifies some relevant aspects:

- Art.34 states that an information assurance (authenticity availability confidentiality integrity non-repudiation) approach should be followed.
- On the use of tools, art. 36 states that preference shall be given to cryptographic products approved by the council. However, no reference is provided for what concerns compatibility and interoperability requirements when information is shared with non-EC institutions.
- Regarding Communication and Information Systems which need to handle this type of information, art. 37 imposes the requirement, for these CIS, to be accredited for handling EUCI, under the scrutiny of the Commission SAA. Again, nothing is said about CIS of other EU bodies or about tools to share EUCI with that bodies. This part is indeed somehow covered by:
- Art. 52 where is stated that exchange of EUCI with other EUIBAs can be done given the execution of an equivalence check and effectiveness assessment related to the used tools and processes.

Unfortunately, no details are provided in relation to equivalence checks and effectiveness, nor the institution which should take the lead in conducting such and assessment.

The Council note 6074/17 makes a step ahead to cover this point, approving the common approach on sharing EUCI with EUIBAs in a way revamping (2013/488/EU). The Annex of the council note, lists the institutions which currently fall under this common approach:

- Other EU institutions
    - Court of Auditors (ECA)
- EU Decentralised Agencies
    - European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)
    - European Agency for the Management of Operational Cooperation at the External Borders (FRONTEX)
    - European Asylum Support Office (EASO)
    - European GNSS Agency (GSA)
    - European Union Network and Information Security Agency (ENISA)
- Agencies established under Title V, Chapter 2, TEU
    - European Union Satellite Centre (SatCen)
    - European Defence Agency (EDA)
- EU Bodies
    - European Police Office (EUROPOL)
    - The European Union's Judicial Cooperation Unit (EUROJUST)

As the common approach is based on 2013/488/EU, the indication provided are mainly at high level, describing procedures, methodologies, etc. However, from pure, operational, point of view, this still does not solve the issue of being able to share EUCI in an easy and interoperable way.

All other EUIBAs have defined their own set of standards. Actually, the lack of a common set of implementing rules leads to a situation where each EU entity is investing significant efforts, while a coordinated action could lead to a much more efficient and solid approach. Only by looking at the e-mail security standards adopted (see Figure 3), it becomes clear that each organisation is adopting different approaches that are not optimal, leading to a situation where exchange of information between these organisations cannot be considered reliable. The lack of a common approach hinders the deployment of common tools building on an agreed set of controls depending on the security needs of the information to be protected.

A detailed analysis of existing decisions and regulations makes it evident that a common set of rules would enable EUIBAs to work more efficiently for achieving:

1. Improved classification or taxonomy of the legal basis of the rules covering the information security in each organisation. Typically, such bases are founded in Commission Decisions 2015/443, 2015/444, and 46/2017. However, depending on the organisation, they may be expanded or particularized in additional decisions, e.g., EUROPOL security rules.
2. Better cooperation across the organisations considering common definitions, roles, and responsibilities (e.g., Local Security Officer - LSO, Local Informatics Security Officer - LISO, Chief Information Security Officer - CISO). This also applies to persons or entities responsible for granting the authorisation for access to EUCI. Currently, each organisation may potentially adopt different definitions and diverse organisation structure leading to issues when information is exchanged.
3. A shared interoperable inter-institutional classification scheme and marking when exchanging information, allowing for appropriate handling measures to be considered, also to be used in corporate information systems or DLP systems. The overhead to consider an appropriate mapping and understanding is substantially large considering the diversity in place where every organisation may potentially have its own marking and handling instructions, especially for non-classified information. Some organisations may not apply any marking at all. Currently mapping tables must be defined for identifying equivalent levels of information sensitiveness.
4. A common approach to monitor, inspect, assess compliance, and provide assurance that information is appropriately protected, at an equivalent level, across organisations also considering information handled in IT systems. This includes not only sensitive non-classified information but also classified information (EUCI), since currently ad-hoc security of information agreements must be established between all potential organisations needing to exchange information.
5. Define specific provisions relating to contractors' staff carrying out tasks related to security. It is important to define a common approach since contractors and outsourcing is heavily used across EU intuitions, bodies, and agencies.
6. Set overarching rules for the software tools used to communicate non-classified information with a limited need-to-know. Currently, there is no standard tool for the exchange and storage of SNC information, thus it usually depends on the sender / recipient capacities and know-how. As already pointed out, several systems are in use, including ARES, SECEM, web portal, email with PGP encryption, Secure Information Exchange Network Application (SIENA) for EUROPOL, email with encrypted compressed files and the password for the compressed file to be send over, e.g., SMS or telephone.
7. Improve and harmonise rules for exchanging EUCI with other EU entities and third parties, including third country administrations or international organisations. Based on the relevant legal basis), this also should cover the underlying arrangement or agreement and its duration. The same issue is also pertinent for the exchange of EUCI with other EU entities.

2.2.4 Vulnerabilities

A vulnerability that may be exploited by an existing threat is concerned with human or other actors, including processes and procedures, personnel, physical environment, hardware, software, and so forth. Finding vulnerabilities and associating them to threats and assets can be achieved via a plethora of tools and methods, including off-the-shelf or custom tailor vulnerability scanning tools, red teams (penetration testing) and relevant testing guides like the OWASP one, Security Testing and Evaluation (ST&E), code review, and bug bounty campaigns. Such endeavour may start by answering basic questions, i.e., what kind of vulnerabilities are we after?, where and how can we find them?, what are the time-bounds and other constraints of finding them?, and also consider face-to-face interviews with users, that is, exploitation of end-users as sensors, questionnaires, offline audit trail analysis, and others. A coarse list of vulnerabilities categorized in three axes, namely physical, administrative, and technical, is presented in Table 3.

Table 3. Categories of vulnerabilities.

Type	Description
Physical	Physical security aspects, including administration areas, secured areas, etc. (out of scope of this report).
Administrative	Inadequate security awareness and knowledge. Inadequate information security management. Inadequate risk management and communication. Missing management support, resources, and finance. Smaller entities cannot implement state-of-the-art technology to protect information due to cost/knowledge issues. Openness, attitude, and culture. Identity management. Lack of unified security policies. Weak cooperation between institutions, bodies, and agencies. Inconsistent security measures between institutions, bodies, and agencies. Paper-focused rules for handling of information. Vetting and clearances are not available or abused. Lack of policies regarding supply chain risk and hardware/software vetting procedures.
Technical	BYOD. Data acquisition, storage, processing, and transfer. Missing best practice security controls. Technical and network complexity. Lack of common tools and procedures for secure exchange of information. Lack of approved and modern cryptographic solutions at the various levels. Lack of secure online places, such as, videoconference services, to discuss/handle EUCI information. Security products are of uneven quality between various EU entities. Lack of common identity repository enabling identification of EUIBAs staff and level of vetting. Cloudification and open network architectures. Outsourced systems. Software vulnerabilities.

2.2.5 Consequences

Consequences are concerned with the manifestation of the upshots an identified threat may inflict, if weaponised by a vulnerability in the context of an information security incident, to its associated list of assets and related processes. This includes damage repair costs, financial and opportunity

costs, loss in reputation, etc. As given in Table 4, the outcomes of this step relate specific incidents with potential harms to the associated assets.

We identify eight general categories of incidents, aiming to steal, modify, manipulate, or delete any kind of information. Naturally, the higher the security level of the information, the greater the severity and range of consequences. For instance, if EUCI pieces of information are stolen, then there is a severe impact on the reputation and credibility of the organisation. Most possibly, such an incident will negatively affect the organisation's relationships with other parties. Moreover, depending on the exact content of the stolen data, the inflicted harm may include monetary loss, damage to critical services or the biosphere, and adverse consequences to certain peoples' personal life and career.

Table 4. General categories of incidents. With reference to Figure 4, the consequences per incident is tightly linked to the importance and sensitivity degree of the affected information.

Incident	**Description**
Inadvertent disclosure	Information with limited need-to-know uploaded on a website or blog or social media, mishandled, or sent to the incorrect party through e-mail or other means.
Malware or hacking	Electronic entry by an external party. Data loss or defacement due to malware, spyware, ransomware, brute force, SQL injection, malicious spam, account hijacking, malicious script injection.
Insider	Intentional data breach by a person with legitimate access, say, an employee, contractor, or trainee.
Physical loss	Missing, destroyed, or stolen non-electronic records, such as paper documents.
Portable device	Missing, destroyed, or stolen portable devices, including laptop, smartphone, portable memory device, backup tapes, and other storage media.
Stationary device	Missing, destroyed, or stolen stationary electronic device such as a desktop computer.
Service disruption	Denial of service; Ransomware; Deceptive actions faking an emergency.
Unidentified	Other data breach for which the root cause is unknown. Threat events capitalizing on zero-day exploits, or unknown.

Figure 4 summarizes the types of impact, adversary's profiles, motivations, resources, and methods identified in this report. By combining these diverse elements, a larger number of potential incidents may arise. In the definition of a common set of rules for information security for all EUIBAs, these categories should be considered with respect to the level of protection needed by the information handled and the possible impact to the organisation.

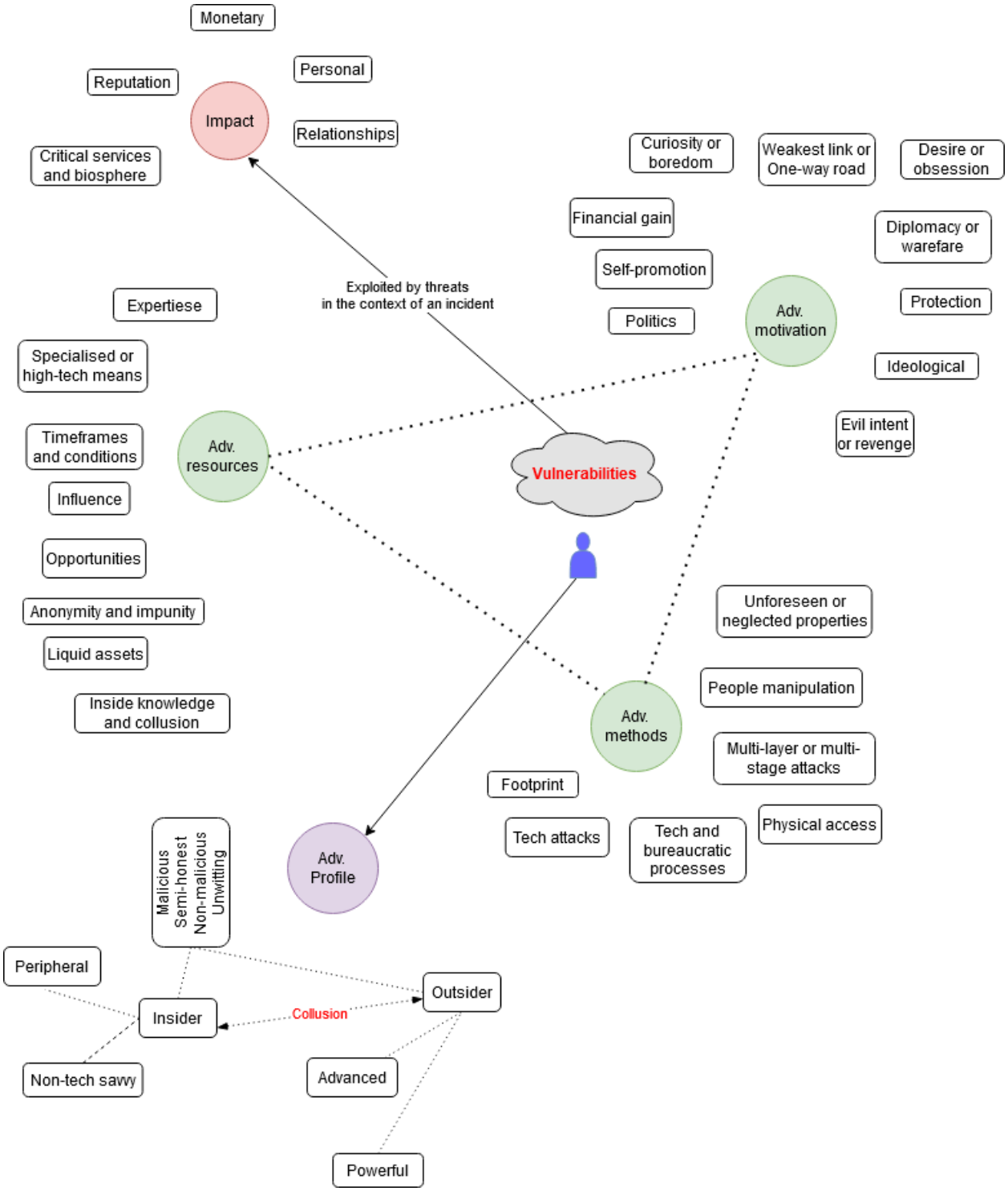

Figure 4. Outline of the threat ecosystem

2.3 Risk analysis and evaluation

The aim of this phase is to grasp the nature, sources, and root causes of the relevant information security risks and estimate their level. The per-risk consequences along with its likelihood vis-à-vis the factors affecting them are studied as well. Information security risk analysis may be qualitative, semi-quantitative, quantitative, or hybrid. As already pointed out in section 0, for the needs of this report, a qualitative approach is chosen. This type of analysis uses descriptive, human-readable scales, e.g., from very low to very high, to characterise the magnitude and likelihood of potential

consequences. The scale employed may be different per risk, and its range is subject to the case at hand.

Based on the analysis done in the previous subsection, we gather in Table 5 key incidents along with the corresponding major vulnerabilities, and threat actors plus an estimation of risk as stemming from the empirically approximated impact and likelihood factors. To exemplify, we also provide a basic risk analysis flowchart for hacking, malware dropping, or deception incident in Figure 5. The projected likelihood estimations shown in Table 5 are supported by the "ENISA Threat Landscape 2020" report [17] and CERT-EU 2020 Q3 EU-I report [4], which conclude to the following key observations.

ENISA

- The most targeted sectors were digital services, government administration, and the technology industry.
- Two of the main identified trends in malicious activity pertain to phishing and ransomware.
- Top 5 motivations: financial, espionage, disruption, political, and retaliation.
- Top 5 wanted assets in order of desire: Industrial property and trade secrets, state/military classified information, server infrastructure, authentication data, and financial data.
- 84% of cyberattacks rely on social engineering.
- 67% of malware was delivered via encrypted HTTPS connections.
- 230K new strains of malware appear every day.
- 71% of organisations experienced malware activity that spread from one employee to another.

CERT-EU

- Targeted intrusion attempts against several EU institutions have been observed. In a couple of cases, the threat actor compromised the VPN services allowing staff to telework.
- A significant number of malware infection attempts against EU institutions has been detected. All of them were orchestrated by major criminal collectives.
- DoS and defacement attacks were slightly on the rise.
- Once more, the COVID-19 outbreak was the most observed subject in generic phishing attacks. Cloud-related phishing also remained significant. Four targeted phishing attempts, using a spoofed EU institution's email address were detected as well. Attackers are also cloning EU institutions network domains to lure victims.
- The discovery of leaked credentials associated with EU staff professional email addresses on publicly accessible repositories remains a major issue, affecting 48 distinct EU institutions.
- A steady number of impersonations of EU official accounts has been detected on LinkedIn, Facebook, YouTube, Twitter, and Instagram.

Table 5. Correlation of major categories of incidents with vulnerabilities, threat actors, and assets. An indicative estimation of impact, likelihood, and risk vis-à-vis the assets of interest is also provided. Note that the list of vulnerabilities per incident is not exhaustive.

Incident	**Vulnerabilities**	**Actors**	**Asset**	**Impact**	**Likelihood**	**Risk**
Hacking and malware	Missing or weak security controls Security awareness Security culture Weak or poorly managed credentials	Cybercriminals State-sponsored actors	EUCI SNC Internal information Public information	Critical High Medium Low	Very high	Very high

	BYOD Complexity Security policy fragmentation Outsourced systems Cloudification Weak cooperation between parties Supply-chain-oriented		Archives	Medium		
Social engineering and targeted attacks	Security awareness Security Culture Missing or weak security controls Human factors	Cybercriminals State-sponsored actors	EUCI SNC Internal inf Public inf Archives	Critical High Medium Low Medium	Very high	Very high
Unintended disclosure and human errors	Security awareness Inadequate security management Security culture Data acquisition, storage, processing, and transfer Complexity BYOD Human factors Weak cooperation between parties	Insiders	EUCI SNC Internal inf Public inf Archives	Critical High Medium Low Medium	High	High
Device or document loss or theft	Insufficient security management Physical security Human factors Vetting and clearances	Cybercriminals Opportunists Insiders	EUCI SNC Internal inf Public inf Archives	Critical High Medium Low Medium	High	High
User account hijack	Security awareness Password security BYOD	Cybercriminals State-sponsored actors Opportunists	EUCI SNC Internal Public Archives	Critical High Medium Low Medium	High	High

		Insiders				
Data abuse or misuse	Inadequate security management Security culture Missing security controls BYOD Security policy fragmentation Vetting and clearances Complexity Weak cooperation between parties	Insiders Opportunists	EUCI SNC Internal Public Archives	Critical High Medium Low Medium	High	High
Insider attacks	Insufficient security management Missing security controls Vetting and clearances	Insiders	EUCI SNC Internal Public Archives	Critical High Medium Low Medium	High	Very high
DoS	Inadequate security management Inadequate resources and finance Missing security controls Complexity Cloudification and open network architectures. Outsourced systems	Cybercriminals Opportunists Hacktivists	EUCI SNC Internal Public Archives	Low Low Low Low Low	High	Medium
Side-channels[10]		Cybercriminals State-sponsored actors Insiders	EUCI SNC	High High	Low	Medium

[10] Attacks aiming to extract secrets from an electronic equipment or a system, through measurement and analysis of physical parameters. Such parameters include execution time, supply current, and electromagnetic (EM) emissions. They can be briefly categorised into timing attacks, power analysis attacks, and EM-attacks.

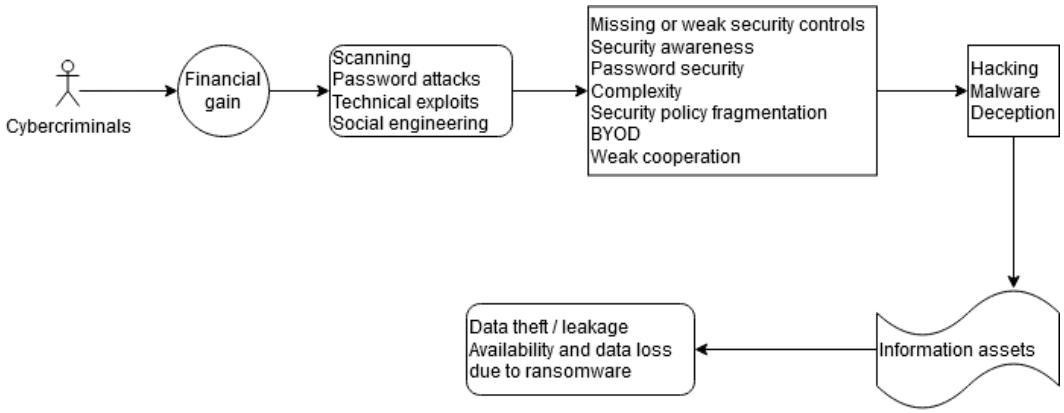

Figure 5. Risk analysis for a hacking / malware dropping / deception incident

On the other hand, the aim of risk evaluation is to offer a side-by-side comparison of the outcomes obtained from the risk analysis stage vis-à-vis the risk criteria defined during context establishment for the sake of facilitating decisions on whether a specified level of risk is admissible or not. In this phase, concrete and justifiable choices must be made regarding which risks are tolerable, and thus currently do not call for treatment, and which of them need to be treated. Treatment priorities associated to the latter category of risks must also be formulated.

With reference to Table 5, it is obvious that the risk associated with EUCI and SNC information is very high, and thus it cannot be admissible; treatment is required. The risk associated with internal information and archives is also significant, but surely of lower priority vis-à-vis the previous. However, this depends on the case, say, some historical documents may present little value to an opponent.

2.4 Risk treatment

Following the discussion from subsection 2.2.3, the risk treatment phase concentrates on risk remediation or mitigation options. Such general options, which may be applied independently or in tandem may be:

1) **Avoiding the risk**, e.g., by removing the affected assets or ceasing/cancelling the associated processes.
2) **Modifying the risk** by introducing controls that, say, remove the source of the risk (correction or elimination), alter the consequences of the risk (impact minimisation), change the probabilities of the risk (prevention, deterrence, detection, recovery, etc.).
3) **Sharing the risk**, but typically not the corresponding liability, with others, i.e., external parties. Normally, this is done either by insuring the asset of interest with a (cyber) insurance company or by outsourcing the implementation and management of a given control, say, the intrusion detection task is assigned to a partner.
4) **Accepting the risk** if it is deemed to satisfy the risk acceptance criteria as they were defined during the context establishment phase.

The first option can be potentially applicable to historical documents (archives). For instance, old enough digital documents and associated data may be taken offline. Both options 3 and 4 fall out of scope of this report. In the following, the focus is on the second option, which is generally the obvious choice for most IT risks. As shown in Table 6, the possible panoramic remedies are concentrated on vulnerability mitigation, which in turn leads to diminishing the probabilities of the risk. As a general guideline, EUCI should be at least moved onto a separate network with more secure access controls.

Table 6. Possible directions on vulnerability mitigation.

Vulnerability	**Treatment**
Inadequate security awareness and knowledge.	Security policies and awareness training in the organisation. Train users to be security sensors. Assessment visits.
Inadequate information security management.	Apply the least privilege (minimality) and separation of duties principles. Defence in depth. Improve procedures. Inspection and audit service. Security throughout the communication and information system life cycle. Incident response. Threat intelligence. Security accreditation authority. Information assurance authority.
Inadequate risk management and communication.	Establish a holistic risk-oriented ISMS. Develop a cyber-threat intelligence program.
Missing management support, resources, and finance.	Common framework contracts / procurement. Common security tools. Inspection and audit service; risk shared with information security.
Openness, attitude, and security culture (cultural aspects pertaining to low tolerance for security rules and low-graded loyalty to administrative policies).	Security policies and awareness training,
Inadequate, obsolete, or fragmented identity management policies.	Improve procedures. Security training. Adopt usable security. Multi-factor authentication. Federation models, e.g., single sign on (SSO) for certain services. Modern identity management schemes, including PKI and distributed ledger technology. Biometrics (for EUCI).
Lack of unified security policies.	Harmonise frameworks for SNC.

	Improve procedures.
Weak cooperation between institutions, bodies, and agencies.	Formal cooperation procedures. Stronger single governance.
Inconsistent security measures between institutions, bodies, and agencies.	Adopt common terminology and practices. Security training. Assessment visits.
Paper-focused rules for handling of information.	Harmonise rules on teleworking and digital workplace. Security training.
Vetting and clearances are not available or abused.	Common rules across all EU entities concerning the clearance procedure. Separation of duties. Assessment visits.
BYOD.	Unify and improve policies and procedures. Security training.
Data acquisition, storage, processing, and transfer.	Unify and improve policies and procedures. Security training. Assessment visits.
Missing best practice security controls.	Develop best practice security controls. Security training.
Technical and network complexity.	Focus on simplification, clarity, and usability. Adopt usable security.
Lack of common tools and procedures for secure exchange of information.	Review the various inter EUIBAs security services. Not only a legal issue (budget and cooperation is required)
Lack of approved and modern cryptographic solutions at the various levels.	Common encryption tool – creation of a framework for an EU trust list. Crypto approval authority.
Lack of secure online places, say, videoconference services, to discuss/handle SNC information.	Set minimum security requirements for dedicated online meeting rooms. In-house installed and maintained open-source secure solutions for teleworking, e.g., Matrix[11]
Security products are of uneven quality between various EU entities.	Common mandatory inspection program.

[11] https://matrix.org/

	Conduct vulnerability assessment.
Lack of common identity repository enabling identification of EUIBAs staff and level of vetting.	Common approach on identity management.
Software vulnerabilities.	Updating and patching. Conduct vulnerability assessment. Software vetting. Sandboxing.
Cloudification and open network architectures.	Minimise exposure of information. Network segmentation. Enforce accountability. On demand or continuous sharing of security incidents and log files. Settle legal issues with external providers and parties. Advanced cryptographic schemes. Secure interconnection of communication and information systems.
Outsourced systems.	Minimise exposure of information. Network segmentation. Enforce accountability. On demand or continuous sharing of security incidents and log files. Settle legal issues with external providers and parties. Advanced cryptographic schemes.
Supply-chain.	Establish relevant policies and procedures. Software/hardware vetting. Evaluation and approval of IT-security products.
Side-channel oriented.	Eliminate or lessen the emission of the leaked (side-channel's) information. Eliminate the relationship between the leaked information and the classified data.

By summarising the generic countermeasures per vulnerability contained in Table 6, one can pinpoint the following key aspects mostly related to IT safeguards.

Training users on information security best practices, apply well-defined reward and accountability, and continuously evaluating and readjusting the information protection ecosystem is important. Also, backing up data, updating and patching software, and implementing incident response and security

management policies are not to be neglected. For instance, taking regular backups is an effective, but frequently disregarded security measure; often restoration from backup is not tested. Two-factor authentication, network segmentation, incident response plans, and log file analysis are also on the very positive side. All these however call for proper information security management, including access control, backup functionality, and integrity checks on classified information. To this end, the establishment of a uniform control and organisation-wide security policies, and a focused strategic alignment is required. For instance, leaving the personnel to devise and follow their own data management systems, say, because a shortcut may seem better, leaves room for diversity in security measures, augments the attack surface, and creates vulnerabilities.

With reference to the current threat landscape as sketched by ENISA and CERT-EU, the following considerations are also of relevance. Patch-level awareness for BYOD is required. Often, devices can enter the network being long time unpatched, while administrators cannot dictate patching. That is, central ICT is incapable of knowing which devices may harm the network and has often little or no control over device-level security. On the other hand, as it is well-known, the primary causes of compromised accounts are password reuse across multiple services, feeble password strength, and low generic awareness. Password aging policy used by many organisations is not a panacea. While it is (still) believed to mitigate the risk by forcing people to change their passwords every, say, 90 days, it imposes unnecessary fatigue, cost, and even provides the illusion of stronger security, while in practice increases risk - the users are simply increment or decrement the number included at the end of their password. On top of that, cultural resistance to security measures for specific persons, a key contributor to insufficient security, is rooted to cultural aspects pertaining to low tolerance for security rules and low-graded loyalty to administrative policies.

All in all, the policies and guidelines should correctly and in simple terms portray proper information management for administrative tasks. The technical systems should be user-friendly and scaled adequately secure to handle the relevant data; usable security is a key issue here. Overall, security management in terms of policy, guidelines, and routines are essential to hinder careless data handling. In this respect, as overarching rules, the list of eight points given in subsection 2.2.3 can be of significant aid.

A limited budget for security infrastructure is one of the main causes for vulnerabilities in organisations where often security investments lag behind other equipment. Moreover, insufficient risk and security incident reporting and poor risk communication channels may also create vulnerabilities. And executive management goals regarding risk management and cyber-defence are on several occasions misaligned to that of those who must implement these strategies and put them into practice.

Focusing on countermeasures, EUIBAs may think of avoiding monolithic solutions, and instead apply an alloy of more aggressive defensive plans and strategies. Also, defensive schemes should be backed up by “offensive” information security strategies and methods, including penetration testing and cyber deception, ultimately leading to the development of “advanced persistence resilience”.

On a more general level, it is important to open a reflection on the current approach related to information classification. Prescriptions, processes, and high-level principles are today seen as silos, where a limited number of generic principles are associated to the different classification levels. This is due to historical reasons, as EUCI information has been for long time, first of all “physical information” to be handled physically and to be preserved “in the real world”, hence with a limited number of scenarios to cover.

With the digitalisation of the EUIBAs, the diversification of information sharing means and underlying technologies, it is becoming more and more difficult to maintain a coherent set of procedures with this monolithic approach. The biggest obstacle is indeed the speed of evolution of technologies which in a way makes difficult to keep the measure in place up-to-date (requiring in fact to have in place a team able to constantly revise them), risking instead to become an obstacle to information sharing, treatment, and analysis.

This limitation is further amplified when information is required to be shared among institutions which are not falling under the same "family", i.e., with common principles, but different implementations.

As at the end the vulnerabilities to which EUCI is exposed are, in the majority of the cases, related to the implementation of the security principle and prescriptions, especially when the principles are in common, a better and more flexible approach would be that of adopting a risk assessment process in the current EUCI rules.

A similar approach, on a side would allow to adapt EUCI rules in a dynamic way based on the context, and on the other would allow to identify the best cross-institution sharing option, without being constrained by pre-constituted and immutable rules.

This option obviously does not come without a cost: a suitable risk assessment and "risk management" framework will need to be defined, tested, implemented, and recognised by all the EU body institutions. However, it has also to be underlined that a similar approach, would also help in the harmonisation when considering EUBA-MSs communications as it would enable a more flexible, precise (hence more secure), and right-to-the-point mechanism for EUCI handling.

3 Conclusions and the way ahead

The risk assessment presented in this report illustrates the complexity and challenging context on which EUIBAs operate within. The digital transformation, the so-called new norm imposed by the COVID-19 pandemic, the shared information security challenges, and the new missions assigned to EU entities can only be efficiently addressed if a well-defined common set of information security policies and rules are in place.

Generally, data is a risky asset. The reality has long proven this. On May 2015, "a sophisticated organised crime syndicate used the IRS website to steal tax forms full of personal financial information on 104K taxpayers" [18]. Especially in the COVID-19 era, risk related to data breaches must not be downplayed; the effects can be calamitous [19], [20]. Large repositories of data with limited need-to-know are very alluring, desirable targets for every criminal and nation-state actor.

While in the big data era, where almost every organisation is tempted to preserve and capitalise on as many data they can, there is no safer option from keeping and exchanging only the portion of data that are deemed necessary; nothing more. Even for the preserved data, there are certain options than can greatly aid in subtracting a certain amount of toxicity in terms of risk, meaning cancelling out motivations, reducing the attack surface, and hardening the defences at the very beginning. Undoubtedly, EU organisations are expected to frequently exchange non-classified and classified information with both other EU and non-EU entities to function efficiently, and therefore comprise a challenging environment exposing a large attack surface in this respect.

From an IT perspective, moving historical data offline, encrypting it, anonymizing data fields, and stripping off superfluous or needless data fields are in the positive direction. And while perfect anonymisation is unattainable in principle, its cost for a potential adversary can be quite high. Moreover, a general distinction can be made; information "assets" versus information "liabilities". The former present value to the organisation, while the latter are pieces of information which are required for operational reasons, e.g., employee PII. So, a goal should be to at least lower the latter to a bare minimum. This is in line with the principles of the European eGovernment Action plan[12], where data should be provided once only and re-used whenever necessary respecting data protection rules.

On the other hand, using online services, i.e., SaaS instead of in-house solutions puts information with a limited need-to-know at risk. Colloquially, "There is no cloud; it's just someone else's computer". Today, using cloud services is almost unavoidable. However, this should be done for services and data which are not deemed classified or, in case data with a limited need-to-know is exchanged, a specific set of well-defined and unified controls should be put in place to greatly mitigate the risks involved.

As already pointed out, from a high-level view, a number of shortcomings can be identified for the handling and communication of information in EU organisations. Those are mostly attributed to the diverse categories of information triggering disparate handling procedures, the lack or limited interoperability of the communication and information systems for EU classified and non-classified information, shortage of consistent rules for non-classified information with a limited need-to-know, and the non-harmonised exchanges of information between EU entities.

All these points indeed find confirmation in the results of a survey recently conducted by HR-DS addressed to EUIBAs, where in many cases a centralised handling of reference security services, accreditation of CIS, clearance and procurement of physical security material were identified as beneficial to enhance the secure sharing and collaboration across the different institutions. Particularly, in the survey emerged how the landscape of reference security services is scattered, many adopt those recognised by the council, but without any officiality, and in many cases interoperability resulted to be an issue. From the same survey emerged also how accreditation of CIS can be extremely complicated especially for institutions with little staff, as well as agreements between institutions with the aim of sharing classified information is also a long and costly process (between 1-3 years).

[12] https://ec.europa.eu/digital-single-market/en/european-egovernment-action-plan-2016-2020

Following the eight key points of subsection 2.2.3, and with an eye towards a new policy addressing common rules on Information security, one can additionally refer to the following suggestions:

- Definition of a common information security glossary. This will guarantee that all EU organisations share the same terminology and reduce misconception risk.
- A greater harmonisation of the IT tools across EU organisations will be the driving force to a more coherent ecosystem and to a single approach for what concerns information security.
- Centralization of common information security tasks seem to mostly pertain to (a) clearances, (b) procurement of physical security material, (c) reference security services, (d) classification and marking of information, especially the SNC one, (e) information sweeping, (f) accreditation and compatibility of CIS, (g) incident response, (h) cyber intelligence, and (i) training and awareness. Overly segmentation and tailor-made solutions augment the attack surface, create incompatibilities, and increase the associated maintenance costs. For some services, including reference security ones, incident response, and training and awareness a federation model could be more suitable. Such a model enables interoperability and information sharing among semi-autonomous de-centrally organised lines of business, information technology systems, and apps. In such a case, common, harmonised and compatible formats to exchange information or mutual recognition agreements are of need.
- Usable security is of need. Namely, security should be as transparent as possible to the end-user.
- Intensified by the COVID-19 crisis, the shortage of harmonised tools and solutions for teleworkers due to diverse requirements has an adverse impact on inter-institutional collaboration. The solutions developed to support this increased need for remote collaboration should mandate that the information is not carried home, but accessed remotely via approved and secured systems. This should also apply to information processing, transmission, and storage through cloud services.
- Definition of a common classification guide on EUCI. Sharing the same reference for marking categories for SNC information between institutions would also bring value to avoid potential mapping exercise between different lists.

Regarding videoconference services to discuss/handle SNC information, an alternative is to use low-cost, low-risk, in-house installed and maintained, open-source, secure platforms for teleworking, such as Matrix.When looking into the future, a key enabling technology to the information security ecosystem stands out. Namely, during the last few years, blockchain technologies have proved they can be trusted, while at the same time increase efficiency, provide data protection, and transparency. Estonia already capitalises on distributed ledger technology to safeguard its e-gov framework [22]. For instance, Estonia applies the so-called “once-only” principle, meaning that zero records of information are stored twice in the system. This enforces data integrity and enables trusted checks on the history and updates of any information record. Note that the implementation of the aforementioned principle is straightforward when blockchain is utilised.

Generally, the transparency and immutability features of the distributed ledger safeguard from data manipulation, either from outsiders or insiders. This is because the information stored on blockchain ledger is almost infeasible to manipulate or delete, which in turn ensures data integrity. Another prominent example in this context is Lockheed Martin, which was the first U.S. defense contractor to implement blockchain into its protocol. According to [21], this company implements blockchain cybersecurity protocol measures in the engineering systems, supply chain risk management, and software development. For obtaining a more holistic view on the use of blockchain technologies in governmental services, the interested reader can also refer to [23].

No less important, distributed ledger technology can be especially handy for securing classified information. For instance, Estonia’s health records are secured via a blockchain technology called Keyless Signature Infrastructure (KSI), actually an alternative to the legacy PKI. Blockchain can be also employed to get rid of passwords in identity management, thus leading to much lesser social

engineering incidents and identity management headaches in general. That is, by keeping a person's identity on a blockchain, the relevant data becomes immutable, and the same person has full control on the block they inserted. This leads to the so-called self-sovereign identity, an approach that gives individuals full control over their digital identities.

References

[1] ISO/IEC, "ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary." 2018.

[2] EU, "Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU - JOIN/2017/0450," Sep-2017. [Online]. Available: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450. [Accessed: 18-Jan-2021].

[3] EU Directive 2016/1148, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union." Jul-2016.

[4] CERT-EU, Direct threats to EU institutions, Bodies and Agencies. Available: https://media.cert.europa.eu/static/MEMO/2020/TLP-WHITE-2020Q3-Threat_Landscape_Report-Executive-Summary-v1.0.pdf. [Accessed: 02-Mar-2021].

[5] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy, COM/2020/605 final, July 2020.

[6] ISO/IEC, "ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management." 2018.

[7] Tamara Denning, Batya Friedman, and Tadayoshi Kohno, "The Security Cards", University of Washington, 2013, [Online]. Available: http://securitycards.cs.washington.edu/activities.html. [Accessed: 18-Jan-2021].

[8] T. Aven, "The risk concept - historical and recent development trends," Reliability Engineering & System Safety, vol. 99, pp. 33–44, Mar. 2012, doi: 10.1016/j.ress.2011.11.006.

[9] D. Gritzalis, G. Iseppi, A. Mylonas, and V. Stavrou, "Exiting the Risk Assessment Maze: A Meta-Survey," ACM Comput. Surv., vol. 51, no. 1, pp. 11:1–11:30, Jan. 2018, doi: 10.1145/3145905.

[10] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology, NIST Special Publication (SP) 800-53 Rev. 4, Jan. 2015.

[11] ISO/IEC, "ISO/IEC 31000:2018 Risk management." Feb-2018.

[12] Official Journal of the European Union, Council decision of 23 Sept. 2013 on the security rules for protecting EU classified information (2013/488/EU), Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013D0488. [Accessed: 18-Feb-2021].

[13] Malwarebytes, Enduring from home - COVID-19's impact on business security. Available: https://resources.malwarebytes.com/files/2020/08/Malwarebytes_EnduringFromHome_Report_FINAL.pdf. [Accessed: 18-Feb-2021].

[14] Verizon, 2020 Data Breach Investigations Report - Executive Summary. Available: https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf. [Accessed: 18-Feb-2021].

[15] Kaspersky, How COVID-19 changed the way people work. Available: https://www.kaspersky.com/blog/secure-futures-magazine/covid19-homeworking-survey/35396/. [Accessed: 18-Feb-2021].

[16] FBI, FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic. Available: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic. [Accessed: 18-Feb-2021].

[17]ENISA, Threat Landscape 2020, [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents. [Accessed: 29-Jan-2021].

[18]CNN [Online]. Criminals use IRS website to steal data on 104,000 people. Available: money.cnn.com/2015/05/26/pf/taxes/irs-website-data-hack/. [Accessed: 29-Jan-2021].

[19]The Drum [Online]. Cyberattack on TalkTalk racks up £60m in damages and loss of over 101k customers. https://www.thedrum.com/news/2016/02/02/cyber-attack-talktalk-racks-60m-damages-and-loss-over-101k-customers. [Accessed: 29-Jan-2021].

[20]Infosecurity Group, Almost Half of Businesses Hit By COVID-Related "Business Impacting Cyber-Attack" in 2020, [Online]. Available: https://www.infosecurity-magazine.com/news/businesses-covid-attack/. [Accessed: 19-Feb-2021].

[21] Builtin, 19 examples of blockchain cybersecurity at work, [Online]. Available: https://builtin.com/blockchain/blockchain-cybersecurity-uses. [Accessed: 19-Mar-2021].

[22]European Commission 2018, Case Study Report: e-Estonia, [Online]. http://www.jiip.eu/mop/wp/wp-content/uploads/2018/10/EE_e-Estonia_Castanos.pdf>. [Accessed: 19-Mar-2021].

[23]Martinovic I., Kello L., Sluganovic I. 2017, Blockchains for Governmental Services: Design Principles, Applications, and Case Studies, [Online]. <https://www.ctga.ox.ac.uk/sites/default/files/ctga/documents/media/wp7_martinovickelloslugan ovic.pdf>. [Accessed: 19-Mar-2021].

List of abbreviations

BYOD	Bring Your Own Device
CDS	Customs Decisions System
CERT	Computer Emergency Response Team
CIS	Communication and Information Systems
CISO	Chief Information Security Officer
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DoS	Denial of Service
EASO	European Asylum Support Office
ECA	European Court of Auditors
EDA	European Defence Agency
EM	Electromagnetic
EMA	European Medicines Agency
ENISA	European Union Network and Information Security Agency
ESA	European Space Agency
ETIAS	European Travel Information and Authorisation System
EU	European Union
EUCI	EU Classified Information
EUIBA	EU institutions, bodies, and agencies
EUROJUST	The European Union's Judicial Cooperation Unit
EUROPOL	European Police Office
GSA	European Global Navigation Satellite Systems Agency
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technology
IoE	Internet of Everything
IT	Information Technology
ITSRM^2	IT Security Risk Management Methodology
LISO	Local Informatics Security Officer
LSO	Local Security Officer
MS	Member State
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RDP	Microsoft's Remote Desktop app
SaaS	Software-as-a-Service
SatCen	European Union Satellite Centre
SECEM	Secure Email

SIENA	Secure Information Exchange Network Application
SIS	Schengen Information System
SIS	Schengen Information System
SNC	Sensitive Non-Classified information
SSO	Single Sign On
ST&E	Security Testing and Evaluation
TLS	Transport Layer Security
VIS	Visa Information System
VPN	Virtual Private Network

List of figures

List of tables

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office
of the European Union