BSA The Software Alliance

EU Cybersecurity Dashboard

A Path to a Secure European Cyberspace

galexia

CONTENTS

EXECUTIVE SUMMARY 1

Methodology 2

KEY FINDINGS 4

Legal Foundations 4

Operational Entities 5

Public-Private Partnership 6

Sector-Specific Cybersecurity Plans 6

Education 6

EUROPEAN UNION CYBERSECURITY MATURITY DASHBOARD (2015) 8

EUROPEAN UNION CYBERSECURITY COUNTRY SUMMARIES 11

EXECUTIVE SUMMARY

The promise of today's interconnected world is immeasurable. Technology has become integral to virtually every sector of the global economy, including banking, communications and the electrical grid. The benefits that stem from that promise, however, face very real threats.

Attackers — in ever greater numbers and with increasing sophistication — see, in the growing promise of our tech-connected world, opportunities to steal or cause major disruption or destruction by exploiting vulnerabilities. Unfortunately, as technology's benefits expand and evolve, so too will the threats. Countering those threats and ensuring the resilience of our cyber-enabled systems will require flexibility and an ability to evolve as well.

For governments, protection from cyber-attacks — as well as the ability to both mitigate the harms of any such instances and to address all newly emerging threats — can be found in the cybersecurity policies they adopt and execute. Three elements must be present: the proper legal and policy frameworks along with the appropriate public input and the necessary infrastructure needed to implement those frameworks.

Laws, rules, institutions and appropriate structure to facilitate cooperation with relevant stakeholders are the key foundations that support countries, as well as non-governmental actors in their effort to protect their systems and prevent, mitigate and respond to cyber-attacks.

Such policy and legal frameworks and appropriate implementation structures must be stable and clear, but they need also to remain flexible. They must take into account and be able to adjust to the evolving threat environment that is inherent in the technology arena.

The purpose of this report — the first-of-its-kind BSA EU Cybersecurity Dashboard — is to provide government officials in each of the EU Member States with an opportunity to evaluate their country's policies against these metrics, as well as their European neighbors.

The most important takeaways of the report can be summarised as follows:

- Most EU Member States recognise that working toward cybersecurity and cyber resilience — with particular focus on the protection of critical infrastructure — should be an important national priority.
- Considerable discrepancies exist between Member States' cybersecurity policies, legal frameworks and operational capabilities, creating notable cybersecurity gaps across Europe.

In addition to this report, the detailed results of the research are available online — at www.bsa.org/EUcybersecurity.

- While 27 EU Member States have established operational entities, such as computer emergency response teams (CERTs), the mission and experience of those entities vary greatly.
- One notable gap is the lack of systematic cooperation with non-governmental entities and public-private partnerships: a well-established framework in place for such partnerships exists in only five EU Member States. This leaves a large area untapped for effective, voluntary collaboration between governments and the private sector that owns and operates the majority of commercial critical infrastructure services in Europe.
- Achieving a coherent approach and common baseline level of cybersecurity in the EU will require a sustained effort. The Network and Information Security (NIS) Directive and its implementation presents an opportunity to focus on protecting Member States' most critical services and assets. Doing so would enable the NIS Directive to play a key role in closing Europe's cybersecurity gap.

This year's report, thus, highlights some fundamental challenges as well as significant opportunities for improving cybersecurity across the EU. If EU Member States can align their approach to cybersecurity and bring their capabilities to a comparable, coherent baseline level, it will be a major step towards achieving a true Digital Single Market in the EU.

Cybersecurity and cyber resilience are often thought of as a funding challenge, but primarily it is a management one. Getting the right policy, legal and operational frameworks in place, improving collaboration with various relevant stakeholders' communities, effectively sharing meaningful cybersecurity information and prioritising the protection of critical infrastructures are key steps which will increase cybersecurity and cyber resilience of all EU Member States.

In addition to this report, the detailed results of the research are available online — at www.bsa.org/EUcybersecurity.

Just as cybersecurity is an ever-evolving field, this report is also intended to be a living document. As national governments and decision makers update their frameworks to address the remaining gaps, this website will be updated to show progress across the relevant areas. We invite you to review these results and contact BSA | The Software Alliance with information regarding any relevant changes.

METHODOLOGY

This study is based on an assessment of twenty five criteria across five themes. (See results, pages 8–9.) Each of the criteria are given a "Yes", "No", "Partial", or "Not Applicable" status. There are no overall rankings or scores in this study.

This analysis is the result of desk-based research on publicly available information, and did not involve direct interviews with national agencies. Where possible we have included links to further information and resources. These are available on our homepage.

The research period concluded on 1 January 2015 and general information in the report is correct up to that date.

For detailed information on the methodology used, please visit our website www.bsa.org/EUcybersecurity.

THE BUILDING BLOCKS OF A STRONG LEGAL CYBERSECURITY FRAMEWORK

Construct Solid Legal Foundations

Governments should enact and keep up-to-date a comprehensive legal and policy framework, based on a solid national cybersecurity strategy. This framework should be built upon the following key principles.

- **Risk-based and prioritised:** Cyber-threats come in many shapes and magnitudes with varying degrees of severity. Establishing a hierarchy of priorities — based on an objective assessment of risk — with critical assets and/or critical sectors at the top is an effective starting point from which to ensure that cyber protections are focused on those areas where the potential for harm is greatest.
- **Technology-neutral:** A technology-neutral approach to cybersecurity protection is vital to ensure access to the most secure and effective solutions in the marketplace. Specific requirements or policies that mandate the use of certain technology only undermine security by restricting evolving security controls and best practices and potentially creating single points of failure.
- **Practicable:** Any strategy is only as effective as it is adoptable by the largest possible group of critical assets and implementable across the broadest range of critical actors. Overly burdensome government supervision of private operators, or disproportionately intrusive regulatory intervention in their operational management of cybersecurity risk would most often prove counterproductive, diverting resources from effective and scalable protection to fragmented administrative compliance.
- **Flexible:** Managing cyber risk is a cross-disciplinary function and no one-size-fits-all approach exists. Each industry, system and business faces distinct challenges, and the range of actors must have flexibility to address their unique needs.
- **Respectful of privacy and civil liberties:** Security requirements should be duly balanced with the need for protection of privacy and civil liberties. Ensuring that requirements and obligations are proportionate, do not represent more intrusion in fundamental rights than what is strictly necessary, follow due process and are supported by adequate judicial oversight are all important considerations to address in any cybersecurity framework.

Establish Operational Entities with Key Responsibilities for Security

Governments should set up operational entities to support the prevention of cybersecurity incidents and to ensure response to them. A core component of this is the establishment of operational computer security, emergency and incident response teams.

Engender Trust and Work in Partnership

No country or government can address cybersecurity risk in isolation. Collaboration with non-governmental entities as well as with international partners and allies is a crucial component of an effective approach to cybersecurity.

- **Partnering with the private sector:** Most infrastructure is owned by the private sector, making effective public-private cooperation essential. Cooperation also improves the effectiveness of risk management by improving the sharing of information, experience and perspective of multiple sources. Particular efforts are needed to foster trust and avoid legal obstacles that may hinder it.
- **Global rather than isolated:** Given that cyber threats are global, effective cybersecurity policies and strategies need to maintain an international outlook, building on joint efforts with partners and allies. They should also leverage international, voluntary and market-driven standards in order to maximise pan-regional and global information sharing and protection.

Foster Education and Awareness About Cybersecurity Risk

People, process and technology are equally important to ensuring cybersecurity. Even the best technology will be ineffective if not used appropriately. Awareness raising, education and training about clearly articulated cybersecurity priorities, principles, policies, processes and programs are essential components of any cybersecurity strategy.

KEY FINDINGS

Recent high-profile cybersecurity incidents have underlined the crucial importance of strengthening cyber resilience in general, as well as the protection of critical infrastructure from cyber threats, both in Europe and around the world. In order to achieve these goals, public and private stakeholders need to be equipped with the capacity to effectively prevent, mitigate and respond to cyber-attacks and incidents.

With an increasing focus on improving cyber resilience in both the Member States and at the EU level, this report — the first-of-its kind BSA EU Cybersecurity Dashboard — provides a comprehensive overview of the state of the current cybersecurity frameworks and capabilities.

As detailed below, the report examines five key areas of each EU Member State's cybersecurity policy environment:

- Legal foundations for cybersecurity;
- Operational capabilities;
- Public-private partnerships;
- Sector-specific cybersecurity plans; and
- Education.

LEGAL FOUNDATIONS

Policymakers have a key role to play in ensuring that both public and private entities are well equipped to face the cybersecurity challenges of an ever more connected world. They can achieve this not only by establishing appropriate legal and policy frameworks, but also through promoting cybersecurity awareness and cooperation with the different actors involved in working towards cyber resilience.

A key component, and in many ways the foundation, of this framework is a national cybersecurity strategy, which is critical for managing national level cyber risks and developing appropriate legislation to support those efforts. A strong cybersecurity strategy should be a "living document," developed and implemented in partnership with key public and private stakeholders. It should contain clearly articulated principles and priorities that reflect societal values, traditions and legal principles.

In this regard, there is a need for further improvement within the EU. Only 19 of the 28 Member States have more or less detailed and comprehensive cybersecurity strategies in place, while eight have not declared any such framework at all. Even in the case of those countries with adopted cybersecurity strategies, the quality of these is variable, many remaining vague and high-level, lacking a clear implementation plan.

Furthermore, most of these documents seem static. Only a small number of countries have already revised and improved their initial strategies and published an updated one. Finally, only a minority of the Member States have reinforced their cybersecurity strategy with relevant legislative and policy instruments that address security, information classification obligations and critical information infrastructure protection requirements.

Policymakers have a key role to play in ensuring that both public and private entities are well equipped to face the cybersecurity challenges of an ever more connected world.

Governments also should assess and establish clear priorities among the critical services and infrastructures that most need protection. Not all assets, systems, networks, data and services are equally essential. Accordingly, it is important that decision makers assess the national infrastructure, based on objective criteria and subject to public comment, and determine those that are providing critical services and functions, whose compromise, damage or destruction through a cybersecurity incident could have national significance.

The results of this study show that more than half of the EU Member States have not yet gone through this evaluation process in order to pursue a strategy or plan to protect their most important assets.

Once these critical infrastructures are identified, their cyber resilience needs to be evaluated in order to identify and address vulnerabilities and gaps.

Best practices developed in the private sector often include systematic internal and third party audits to test the cyber resilience of critical systems. This approach is equally valuable for the public sector, yet the study has shown that most EU Member States and public bodies do not follow such best practices.

Finally, as discussions around mandatory cyber incident reporting intensify, it is important to note that **most European countries seem to remain reluctant to introduce such schemes, many of them favoring formal or informal cooperation with the private sector**. Many fear that a mandatory requirement to notify incidents may be less effective than the exchange of information based on mutual trust and ongoing collaboration.

Indeed, if a notification regime should be introduced, most Member States recognise the importance that only incidents having a significant impact or causing a serious risk of harm should be captured by the obligation.

Sharing cybersecurity relevant information is no doubt an important aspect of an effective approach to cyber resilience, as it serves the interest of both public and private stakeholders. This is because it increases collective awareness and, thereby, enables every stakeholder to adapt their security posture to the evolution of the threat landscape.

Effective information sharing, however, requires information protection, appropriate information classification requirements are therefore crucial. This is recognised by almost all EU Member States as most of them have such classification requirements in place.

Governments also should facilitate information sharing by supporting the creation of public-private partnerships and sector-specific collaboration (see below), as well as by providing the necessary human and technical resources, operational entities and the appropriate legal protections against anti-trust claims, undue disclosure requirements or liabilities, and identify and address any other policy and legal barriers that may inhibit information sharing.

OPERATIONAL ENTITIES

Incident-response capabilities should be established to manage the most critical and significant events that threaten the confidentiality, integrity or availability of nationally significant information networks and systems. Computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs) can play a crucial role in improving cyber resilience.

These bodies can provide incident response services to victims of attacks; share information concerning vulnerabilities and threats with key stakeholders in the government, private sector and in some instances with the broader public; and offer other ways of helping to improve computer and network security.

Effective partnership between public and private sectors is all the more important because non-government entities manage and operate many critical infrastructures that we rely on every day, including those that control transportation, health, banking and energy.

Given this important role, it is a positive development that most EU Member States have operational CERTs, with only Cyprus and Ireland yet to make their CERTs fully operational.

Most of the countries also have established competent national authorities for network and information security.

PUBLIC-PRIVATE PARTNERSHIP

The culture of cybersecurity requires collaborative efforts and coordination among all national stakeholders. Effective partnership between public and private sectors is all the more important because non-government entities manage and operate many critical infrastructures that we rely on every day, including those that control transportation, health, banking and energy.

While the importance of cooperation is recognised in Europe, there is a wide diversity in national approaches and maturity levels on this issue. Five countries — Austria, Germany, the Netherlands, Spain and the United Kingdom — are leading the way by having established formal public-private partnerships for cybersecurity.

On the other hand, public-private partnerships for cybersecurity are either non-existent, very restricted, or still at a very early stage of development in the majority of the Member States.

SECTOR-SPECIFIC CYBERSECURITY PLANS

While certain elements of cybersecurity protection apply across all areas, and a wide variety of recommendations are available from national and international organisations, there is also a need for guidance that is tailored to the business needs of particular entities or provides methods to address unique risks or specific operations in certain sectors.

Moreover, while there is a growing interest in establishing sector-specific responses to cybersecurity, practical implementation is still fairly limited in the Member States. The same countries that are leading the way in public-private partnerships also are the leaders in this field, often establishing sector-specific dialogues and information exchanges with the private sector. Such steps can help promote the most suitable and effective guidance throughout individual sectors.

EDUCATION

No single entity or group of stakeholders can secure cyberspace alone — and no individual or group is without responsibility for playing a part in cybersecurity. As not only governments, but organisations of all sizes, as well as consumers, need to take steps to secure their own systems, education and awareness raising play a crucial role.

This requires educational and awareness-raising campaigns as well as support for the development and generalisation of cybersecurity training in universities and in earlier curricula.

The European Union has expressed a strong commitment to cybersecurity education and awareness raising and is acting upon this commitment. For instance, the European Cyber Security Month takes place every October all over Europe, with most EU countries participating.

On the other hand, a small number of countries, including Greece, Malta, Portugal and Slovenia have yet to implement national education strategies in this field.

STUMBLING BLOCKS IN THE PATH TO TRUE SECURITY

Some governments today are invoking cybersecurity as a justification for a variety of policies that go beyond what is needed to address legitimate security concerns. In fact, such policies often undermine cybersecurity rather than improve it. They also impose unfair market access barriers on global producers and service providers, whether intended or not.

Avoid Unnecessary or Unreasonable Requirements

A proper cybersecurity policy enables organisations to develop and adopt the widest possible choice of cutting-edge cybersecurity solutions. It also allows entities to implement the security measures that are most effective at mitigating the specific risks they face.

Some governments instead impose various requirements that restrict choice, increase costs and reduce the ability of their own firms to use the most appropriate cybersecurity tools available. These include, but are not limited to, country unique certification conditions or local testing requirements; mandates for local content; requirements to disclose sensitive information, such as source codes and encryption keys; and, restrictions on foreign ownership of intellectual property.

Refrain from Manipulating Standards

Technology standards play a vital role in enabling and enhancing cybersecurity. By supporting internationally recognised technical standards that are developed with industry participation and accepted across markets, companies can more quickly develop and distribute newer and more secure products.

Even so, some governments have imposed country-specific standards with the argument that requiring market-specific rules will lead to improved cybersecurity. The real effect, however, is the opposite. Government-imposed standards, rather than bolstering security, tend to freeze innovation and force consumers and businesses into using products that might not suit their needs.

Avoid Data Localization Rules

With the rise of global cloud computing services, companies of all sizes around the world can leverage powerful resources that were once available only to the largest firms. The cloud model, though, is based on networks that allow the storage and processing of data in multiple locations and even in multiple countries. By allowing data to flow freely among multiple markets, cloud providers can deliver numerous advantages, including reliability, resiliency, and 24-hour service support.

Based on the mistaken assumption that data is safer in a specific location, some countries are imposing rules that prohibit or significantly impede data transfers across borders. Policies that unnecessarily restrict the free flow of data undermine the very benefits of cloud computing by increasing costs and threatening to prevent access to emerging cloud-enabled services.

Avoid Preferences for Indigenous Technologies

Cutting-edge products and services are developed through global collaboration in research and design centers in many different countries. Countries should create incentives for cross-border collaboration to facilitate voluntary technology transfer and the rapid development and deployment of enhanced products and services.

However, some countries take the opposite approach, assuming that by preventing foreign competition they can protect domestic champions, develop an indigenous technology industry, and enhance cybersecurity. By definition, indigenous technologies are a subset of global innovation. Preventing foreign competition reduces cybersecurity by denying firms and agencies from buying world-class products and services. Furthermore, such policies deprive domestic technology firms of valuable opportunities to collaborate with global leaders and make them less competitive internationally, harming global innovation.

EUROPEAN UNION CYBERSECURITY MATURITY DASHBOARD (2015)

✔ Yes ✖ No ◑ Partial

#	QUESTION	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France
	LEGAL FOUNDATIONS										
1.	Is there a national cybersecurity strategy in place?	✔	✔	✖	✖	✔	✔	✖	✔	✔	✔
2.	What year was the national cybersecurity strategy adopted?	2013	2012	–	–	2013	2011	–	2014	2013	2011
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	◑	◑	✖	✖	✔	✖	✔	✔	✖
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	✖	✖	✖	✖	✔	◑	✔	◑	✖
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	✔	✔	✔	◑	✔	✔	✔	✔	✔
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✔	✖	✖	✖	✖	◑	✖	✔	✔	✖
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◑	✖	✖	◑	✖	✔	✖	✔	✔	✖
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	◑	✖	✖	✔	✔	✖	✔	✖	✖
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	✔	✔	✖	✖	✔	✔	✔	✔	✖
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	◑	N/A	N/A	N/A	◑	✔	✔	✔	◑
	OPERATIONAL ENTITIES										
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔
2.	What year was the computer emergency response team (CERT) established?	2008	2008	2008	2009	–	2011	2009	2008	2014	2008
3.	Is there a national competent authority for network and information security (NIS)?	◑	✔	✔	✔	◑	✔	✔	✔	✔	✔
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔
5.	Are national cybersecurity exercises conducted?	✔	✔	✔	◑	◑	◑	✔	✔	✔	✔
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	✖	◑	✖	✖	✔	◑	◑	✖	✖
	PUBLIC PRIVATE PARTNERSHIPS										
1.	Is there a defined public private partnership (PPP) for cybersecurity?	✔	◑	◑	◑	◑	✖	✖	◑	◑	✖
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✔	✔	◑	✖	✖	✖	✔	◑	✔	✖
3.	Are new public private partnerships in planning or underway (if so, which focus area)?	✔	–	✖	✖	✖	◑	✖	✖	✖	◑
	SECTOR SPECIFIC CYBERSECURITY PLANS										
1.	Is there a joint public private sector plan that addresses cybersecurity?	✔	✖	✖	◑	◑	✖	✖	✖	◑	✔
2.	Have sector specific security priorities been defined?	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
3.	Have any sector cybersecurity risk assessments been conducted?	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖
	EDUCATION										
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	◑	◑	✖	✖	✔	✖	✔	✔	✔

Germany	Greece	Hungary	Ireland	Italy	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom
✔	✖	✔	✖	✔	✔	✔	✔	✖	✔	✔	Draft	✔	✔	✖	✔	✖	✔
2011	–	2013	–	2014	2014	2011	2013	–	2013	2013	–	2013	2008	–	2013	–	2011
✔	✔	◑	✖	✔	✖	◑	✖	◑	✔	✔	✖	✔	✔	✔	✔	✔	✔
✖	◑	✔	✖	✖	✖	✖	✖	◑	◑	✖	✖	✖	◑	✖	✖	✔	◑
✔	✔	✔	✖	✔	✔	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔
✔	✖	✔	✖	✔	✔	✔	✖	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔
Draft	✖	✖	✖	✖	✔	◑	◑	◑	◑	✖	◑	✖	✖	◑	◑	✖	✖
Draft	✖	✔	✖	✔	✖	◑	✖	✖	✔	✖	◑	✖	◑	✖	✖	✖	◑
✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔	✖
✔	✖	✖	✖	✖	✔	✔	✖	✔	✖	✔	✖	◑	✖	✔	✖	✖	✖
✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔
✔	✔	✔	N/A	✔	◑	◑	◑	N/A	✔	◑	N/A	◑	✖	N/A	✔	✔	◑
✔	✔	✔	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
2012	2009	2013	–	2014	2006	2006	2011	2002	2012	2008	2008	2011	2009	2010	2008	2003	2014
✔	✔	✔	✖	✔	✔	✔	◑	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔
✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
✔	✔	◑	✔	✔	✔	◑	◑	◑	✔	◑	◑	◑	✔	◑	◑	✔	✔
✖	✖	✔	✖	✔	✔	◑	◑	✖	✔	✔	◑	◑	✖	✖	✔	◑	✔
✔	✖	◑	✖	◑	✖	✖	✖	◑	✔	✖	◑	✖	✖	✖	✔	◑	✔
✔	✖	◑	✔	◑	✖	◑	✖	✖	✔	◑	✖	◑	◑	◑	✔	◑	✔
✔	✖	✖	✖	◑	◑	◑	◑	✖	–	✖	✖	✔	✖	✖	–	✖	–
✖	✖	◑	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✔	✖	✔
✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	◑	✖	◑
✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
◑	✖	✔	◑	✔	✔	✔	✔	✖	✔	✔	✖	✔	✔	✖	✔	✖	✔

ESTABLISHING AN APPROPRIATE FRAMEWORK FOR MEANINGFUL INFORMATION SHARING

Cybersecurity incidents or breaches can have a major impact on governments, private entities, as well as individuals. Some high-profile breaches have encouraged governments around the world to consider how to best prevent, detect and react to these incidents.

The exchange and sharing of the appropriate information at the right time — and the coordinated effort among relevant actors it enables — is considered the best way to reduce and mitigate risks and respond to cyber incidents.

Accordingly, the key question is how to best achieve meaningful and effective information sharing among relevant stakeholders. While some countries have considered mandatory incident notification systems, these alone would not suffice to address the issue of collective awareness and preparedness. When it comes to that, voluntary information exchanges based on trust have proved to be the most efficient way to achieve successful information sharing.

Such meaningful information sharing is not an easy undertaking. It can only be achieved if the necessary environment facilitating such exchanges is in place. Some of the fundamentals of such an environment are the following:

- **Create an environment of trust:** Information sharing, as well as incident reporting, require safeguards and incentives for their effective functioning. These elements help ensure the trust necessary for the operation of such a system. They include guarantees that the sharing of information will not subject the organisation providing these to undue liabilities, public humiliation, litigation or sanctions.
- **Ensure a high level of confidentiality:** Given the sensitive nature of the information shared about an incident or cyber threat affecting any critical infrastructure, it is crucial to ensure that confidentiality and security of the communications between the infrastructure operator and any supervisory authorities are respected and maintained, subject to transparent reporting by the authority, as appropriate.

  Nevertheless, in some cases, informing the public of an incident may be necessary. In these instances all care should be taken to ensure an in-depth dialogue between the entities suffering a breach and the authorities before any disclosure in order to avoid increasing the attack surface, multiplying the impact of the incident, creating panic, or leading to undue public shaming.
- **Ensure reciprocity:** While the private sector owns and operates much of the countries' critical infrastructure, information sharing should not be seen as a one-way provision of relevant data from private to public entities. It should be regarded as a real and mutual exchange of information, based on trust and mutual benefits.
- **Make requirements clear and consistent across jurisdictions:** As mandatory notification requirements cover an ever-increasing number of areas and geographies, the likelihood of facing conflicting legal obligations increases. As various organisations operate in multiple sectors across different countries and regions, the questions of what to report when and to whom already pose important compliance challenges. Therefore, to the extent a mandatory notification system should be introduced, it is imperative to strive for as much consistency as possible not only among the different notification obligations, but also among the various national and regional requirements.

EUROPEAN UNION CYBERSECURITY COUNTRY SUMMARIES

The following summaries give an overview of the cybersecurity landscape, based on the set of criteria outlined above, highlighting key cybersecurity legislation and policy, as well as the main entities currently operating within each jurisdiction. For more detailed information on each country surveyed, please refer to the detailed Member State summaries available at www.bsa.org/EUcybersecurity.

AUSTRIA

The Austrian Cyber Security Strategy was adopted in 2013. It is part of a broader ICT security initiative of the Austrian government, as set out in the National ICT Security Strategy 2012. The Strategy is an extensive plan that maps targeted cybersecurity objectives into organised fields of action.

Austria has an established computer emergency response team, CERT.at, with a broad and well-defined scope. There are also several public-private partnerships related to cybersecurity operating in the country, such as the Centre for Secure Information Technology Austria (A-SIT) and Kuratorium Sicheres Österreich.

The Austrian Trust Circles provide formal structures for sector-specific information exchanges related to the critical information infrastructure of various sectors. These platforms are tasked with developing sector-specific risk management plans. The Austrian Trust Circles are an initiative of CERT.at and the Austrian Federal Chancellery.

BELGIUM

Belgium's Cyber Security Strategy was adopted by the government in 2012. The legal framework for cybersecurity in Belgium, however, remains somewhat unclear, and the information available on the implementation of the strategy is limited.

On the other hand, Belgium does have an established computer emergency response team, CERT.be, and a well-developed cybersecurity incident-reporting structure. Belgium also recently announced the launch of a new Cybersecurity Centre. There is active support in the country for public-private partnerships, through BeINIS, a government body that liaises closely with private and semi-private entities.

BULGARIA

The legal framework for cybersecurity in Bulgaria is limited, and there is no national cybersecurity strategy in place. There are also no formalised public-

private partnerships, although a significant number of cybersecurity events and academic discussions are focused on cybersecurity and critical information infrastructure protection.

CERT Bulgaria is the country's most significant cybersecurity entity and the focus of recent efforts from the government to strengthen cybersecurity.

CROATIA

Croatia has yet to establish a comprehensive cybersecurity strategy or a well-developed system of public-private partnerships.

Croatia has two established computer emergency response teams (CERTs). The National CERT, established in 2009 is responsible for coordinating security and incident response measures for parties that use a Croatian IP address or .hr domain. The Information Systems Security Bureau's ZSIS CERT has jurisdiction over Croatian government institutions.

CYPRUS

Cyprus adopted a national cybersecurity strategy in 2013. It includes a commitment to update key elements of the legal framework for cybersecurity. Cyprus also is working toward the establishment of a national CERT, which is expected to be operational in 2015. The country has also taken an interest in sector-specific approaches to the management of cybersecurity, with a potential focus on the energy and financial services sectors.

CZECH REPUBLIC

The Cyber Security Strategy of the Czech Republic for the period 2011-2015 was published in 2011. The strategy provides general cybersecurity principles and clearly stated goals. On 1 January 2015, the Act on Cyber Security came into force. This law includes comprehensive provisions on most aspects of cybersecurity and is complemented by several important regulations.

The country has also established a national CERT, CSIRT.CZ, as well as a CERT dedicated to government agencies: GOVCERT.CZ.

The National Cyber Security Centre was launched on 1 January 2015 to promote public-private partnerships. Furthermore, the Czech Republic is conducting a sector-based security risk assessment in cooperation with the academic and private sectors. The project is the first such assessment that addresses cybersecurity.

DENMARK

Denmark does not have a national cybersecurity strategy or a law dedicated to the subject. Denmark recently passed a law that establishes the Centre for Cyber Security, which both takes control of and supersedes its current government CERT. The scope and powers of the new centre are still to be confirmed.

The Danish private sector has established a formal framework for cooperation on cybersecurity issues through the Council for Digital Security.

ESTONIA

Estonia was one of the first countries to develop a national cybersecurity strategy in 2008, followed by the release of an updated strategy in 2014. The country also has a wide range of legislation that covers information security and cybersecurity. Estonia has a well-established CERT, CERT Estonia, under the control of the Information System Authority. Further to national bodies, also notable is the fact that NATO's Cyber Security Centre of Excellence is based in Estonia.

While no formalised public-private partnerships exist, public entities do work closely with relevant private-sector organisations.

FINLAND

Finland published a comprehensive cybersecurity strategy. It is complemented by a strong overall legal framework encompassing a range of important cybersecurity issues. The national authority responsible for cybersecurity in Finland is in transition, involving the amalgamation of two government CERTs and the creation of the Cyber Security Centre.

FRANCE

France has had a national cybersecurity strategy in place since 2011, although it has a strong focus on defence and national security issues. The National Agency for the Security of Information Systems (ANSSI) is a well-established authority dedicated to information security and is integrated with the country's computer emergency response team, CERT-FR. The cybersecurity strategy contains recommendations for closer cooperation with the private sector, but this has not been significantly developed. ANSSI has published sector-specific security measures, making France one of the few EU countries to adopt such a targeted approach to managing cybersecurity.

GERMANY

Germany has a comprehensive cybersecurity strategy, adopted in 2011 and complemented by a strong cybersecurity legal framework. The existence of the Federal Office for Information Security (BSI), in charge of managing computer and communication security for the German government, is a clear demonstration that cybersecurity is elevated to a high government level. Germany also has a network of CERTs, with the national CERT, CERT-BUND, working closely with both state-level and non-governmental CERTs.

Furthermore, the country has well-developed public-private partnerships, such as the Alliance for Cyber-Security and the UP KRITIS partnership, and its national policies and legal framework reflect this focus on cooperation.

GREECE

Greece does not have a cybersecurity strategy or dedicated cybersecurity legislation. The legal and institutional framework that supports cybersecurity is also limited. The national computer emergency response team, NCERT-GR, is limited to government institutions and operators of critical infrastructure.

There are no significant public-private partnerships in Greece, and the government is not actively pursuing their establishment or closer cooperation with the private sector.

HUNGARY

The National Cyber Security Strategy of Hungary was adopted in 2013. The strategy covers key principles of cybersecurity, an overview of Hungary's current cybersecurity situation, and its future cybersecurity goals. Hungary has a limited legislative framework dedicated to cybersecurity.

Several public authorities play a role in cybersecurity, including the National Security Authority, which deals with information security, and the Cyber Security Centre, part of the intelligence services, which deals with cybersecurity. Hungary also has a computer emergency response team, CERT-Hungary, but its remit is limited to government institutions. Furthermore, while the National Cyber Security Centre is tasked with liaising with the private sector, there are no formalised public-private partnerships.

IRELAND

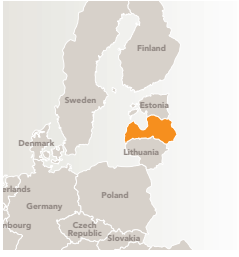
Ireland's national legal and policy framework is very limited when it comes to cybersecurity. A cybersecurity strategy is being developed, but there is no clear timeframe for its release or adoption. Ireland is also one of the few countries in the European Union without an operational CERT, although it is in the process of establishing one.

While there is no formalised public-private partnership set up for cybersecurity, Irish private sector entities, including Infosecurity Ireland, appear to be quite active in this field. In addition, Ireland organised a number of successful individual cybersecurity education campaigns, such as the "Make IT Secure", which included releasing online resources alongside a television advertising campaign.

ITALY

Italy updated its security laws in 2007 and adopted cybersecurity plans in 2013 and 2014, resulting in a strong legal framework supporting cybersecurity. The Italian cybersecurity strategy also calls out public-private partnerships as the intended direction for cybersecurity, but no formalised cooperation yet exists.

CERT-PA was established in 2014. It is responsible for cybersecurity warning systems and the coordination of incident response measures for Italian government institutions.



LATVIA

The Latvian cybersecurity strategy, published in 2014, contains a clear set of concrete objectives matched with specific implementation dates. It also has a strong legal framework for supporting cybersecurity, an important pillar of which is the Law on Security of Information Technology adopted in 2010. This law sets out the roles and responsibilities of the country's national computer emergency response team, CERT.LV.

While the cybersecurity strategy provides for the establishment of formalised public-private partnerships for cybersecurity, no such platforms yet exist.

LITHUANIA

Lithuania published a comprehensive cybersecurity strategy in 2011, however information on its implementation remains limited. The Lithuanian computer emergency response team, CERT-LT, covers all national networks, not exclusively government ones, and the State Information Resources Management Council acts as a powerful policy formation and management body.

The cybersecurity strategy recognises the value and need for public-private partnerships, but no formalised or systematic cooperation yet exist.

LUXEMBOURG

Luxembourg has a fairly limited cybersecurity strategy, published in 2013, which contains some key guiding principles but has little detail on their implementation. The country's legal framework for supporting cybersecurity is also yet to be fully developed. The need to encourage public-private cooperation is a principle mentioned in the cybersecurity strategy, but no formal cooperation is known.

Luxembourg has two CERTs. CIRCL is a response coordinating body that covers all organisations operating in Luxembourg, while GOVCERT.LU is dedicated to public authorities. CASES, a government information security agency, engages in awareness raising activities and the promotion of best practices.

MALTA

Malta has yet to develop a comprehensive legal and policy framework for supporting cybersecurity, although its Digital Malta Strategy and e-government plan promise the elaboration of a cybersecurity strategy.

The Malta Information Technology Agency (MITA) appears to be active in cybersecurity. The national CERT is CSIRT Malta, which is responsible for coordinating incident response measures for entities engaged with Maltese critical infrastructure.

NETHERLANDS

The Netherlands has a sophisticated and mature legal and policy framework for cybersecurity, which includes the National Cyber Security Strategy 2. Adopted in 2013, it is the second such strategy, as the country's cybersecurity framework is renewed every two years.

The Netherlands also has a National Cyber Security Centre, an expanded CERT dealing with all cybersecurity related procedures and practices in a centralised manner. The centre also actively participates in the work of the Information Sharing and Analysis Centres (ISACs) for sectors involved with critical infrastructure.

POLAND

Poland has a comprehensive cybersecurity strategy with clear goals. It was adopted in 2013, thus most of the recommendations are still being implemented. The legal framework for cybersecurity is still not fully developed.

Poland has several CERTs, including CERT.GOV.PL, which covers government and critical infrastructure entities. It also acts as the cybersecurity authority. CERT Polska is an academic CERT covering the entire .pl network in a semi-official capacity.

PORTUGAL

Portugal has not developed a comprehensive legal and policy framework for cybersecurity, and its cybersecurity strategy has not been elaborated. There is no formalised public-private cooperation in place.

The country does have a national CERT, CERT-PT, and the National Centre for Cybersecurity. The latter was established by the National Security Authority and is tasked with liaising with the private sector on cybersecurity incidents.

ROMANIA

Romania has a somewhat vague cybersecurity strategy, adopted in 2013. Its legal framework is limited, although relevant legislative proposals have been submitted to the parliament for adoption. CERT-RO is the national computer emergency response team. It covers all users of Romanian networks. Furthermore, the cybersecurity strategy proposes the establishment of two other cybersecurity agencies.

SLOVAKIA

Slovakia adopted its first, five-year cybersecurity strategy in 2009. Details on the new strategy for 2014 to 2020 remain limited. Slovakia has a CERT, CSIRT.SK, that focuses on government agencies and critical infrastructure operators. There are no defined public-private partnerships for cybersecurity.

SLOVENIA

Slovenia has yet to develop a comprehensive legal and policy framework for cybersecurity. As such, it also has yet to adopt a national cybersecurity strategy. SI-CERT is the national computer emergency response team, and it deals with all Slovenian networks. There are no defined public-private partnerships for cybersecurity in Slovenia.

SPAIN

Spain adopted the National Cyber Security Strategy in 2013. It is a comprehensive document, which sets objectives and targeted lines of actions. It is compatible with, and references, both the National Security Plan and existing security laws; and these plans and laws work together as a package.

Spain has established two CERTs, INTECO-CERT and CCN-CERT, and the National Centre for Critical Infrastructure Protection (CNPIC). The latter appears to be the premier agency for information security and cybersecurity, while the role of the CERTs is limited to dealing with cybersecurity incidents. CNPIC is responsible for ensuring coordination and cooperation between the public and private sector. It also runs sectoral working groups and is working toward the development of sector-specific cybersecurity plans.

Additionally, cooperation with the private sector is formalised through the National Advisory Council on Cybersecurity, established in 2009, whose members are private sector representatives. The council is tasked with providing policy advice to the government, although its current status is somewhat unclear. Private sector associations are also active, with two prominent bodies dedicated specifically to cybersecurity and information security, as opposed to general IT matters.

SWEDEN

Sweden does not have a national cybersecurity strategy, but one is being developed. There are no laws in Sweden that specifically deal with cybersecurity.

Sweden does, however, have a functioning CERT, CERT-SE, which has jurisdiction over all Swedish networks. Furthermore, the Swedish Civil Contingencies Agency (MSB), which is the national authority in charge of information security, has helped Sweden establish a good reputation on cybersecurity. MSG is the centralised information security entity and has a prominent public presence.

UNITED KINGDOM

The United Kingdom has a comprehensive cybersecurity strategy, which was released in 2011. It is complemented by a strong cybersecurity legal framework and two CERTs: CERT-UK mainly supports operators of critical infrastructure while GovCertUK supports government agencies. Other relevant bodies include the National Security Council and the Office of Cyber Security and Information Assurance.

The United Kingdom also has a well-developed system of public-private partnerships in which the private sector actively participates. This collaborative approach also is strongly supported by its cybersecurity strategy. The Centre for the Protection of National Infrastructure (CPNI), for example, organises sector-specific information exchanges, covering 14 sectors.

ABOUT BSA

BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life.

With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

www.bsa.org

BSA Worldwide Headquarters

20 F Street, NW
Suite 800
Washington, DC 20001

T: +1.202.872.5500
F: +1.202.872.5501

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapore 199555

T: +65.6292.2072
F: +65.6292.6369

BSA Europe, Middle East & Africa

2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom

T: +44.207.340.6080
F: +44.207.340.6090