TRANSATLANTIC CYBERSECURITY

Forging a United Response to Universal Threats

U.S. CHAMBER OF COMMERCE

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

SIDLEY

Sidley Austin LLP provides a broad range of legal services to meet the needs of a diverse client base. The strategic establishment of their offices in the key corporate and financial centers of the world has enabled them to represent a broad range of clients that includes multinational and domestic corporations, banks, funds and financial institutions.

This report has been prepared on behalf for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers. The content therein does not reflect an opinion of the firm. Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at www.sidley.com/disclaimer.

TRANSATLANTIC CYBERSECURITY

TABLE OF CONTENTS

1. INTRODUCTION AND EXECUTIVE SUMMARY

The European Union (EU) and the United States are the leading hubs of global information and communications networks that strengthen the deep economic, political, and social ties between these two unions and link each of them with the rest of the world. These networks face cyber threats that are global in origin, indifferent to national borders, and common to both sides of the Atlantic.

Leaders in the EU and United States have recognised that the interconnectedness of information and communications systems and the global nature of the threats demand international cooperation and convergence to tackle cybersecurity risks. In fact, legal and policy measures adopted to address these risks are an area of convergence between the EU and the United States. This report explores this convergence and identifies opportunities to build on it in order to strengthen transatlantic cybersecurity.

The report begins by describing the transatlantic "cybersecurity commons" and the strong economic and security ties that dictate a shared approach to cybersecurity. It then reviews the relevant legal and public policy landscape in the EU and the United States. At the EU level, this consists primarily of legislation that takes effect in 2018: the Network Information Security Directive (NIS Directive) and the General Data Protection Regulation (GDPR). In the United States, the centrepiece is the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework) issued in 2014 and now undergoing revision, coupled with state data breach notification laws and regulation of data security practices by various federal and state laws and agencies.

The report focuses on key points in common among these laws and policies. While there are certain differences between the EU and U.S. legal processes, their approaches to cybersecurity are aligned in essential ways. These converge around voluntary risk-based standards that can be enhanced constantly to reflect metastasizing cyber threats. Both the United States and the EU recognise and wish to encourage robust information sharing among organisations and with governments.

TRANSATLANTIC CYBERSECURITY

This report recommends ways that the EU and U.S. approaches to cybersecurity can be enhanced by adapting the NIST Framework into European cybersecurity frameworks. In particular, EU governmental authorities can incorporate the framework into implementation of the NIS Directive and the GDPR. In addition, EU stakeholders can help refine the forthcoming version of the NIST Framework so as to facilitate its use within the EU. This will, in turn, allow for broader and deeper EU and United States collaboration on cybersecurity both at the governmental level and within the private sector.

Based on points of convergence, the report shows how the NIST Framework provides a proven and effective tool to put into practice objectives of the NIS Directive and the GDPR. Collaboration to incorporate the NIST Framework into implementation of the NIS Directive and the GDPR, as well as broadening the engagement of EU stakeholders in developing the NIST Framework and international stakeholder engagement in implementation of EU legislation, will build on existing convergence and help protect the transatlantic cybersecurity commons. This report proposes a set of concrete recommendations for working towards a common framework, standards, and practices. Cybersecurity is too important to vital common interests for the EU and the United States to speak divergent languages in responding to a common challenge.

Forging a United Response to Universal Threats

Nine Steps to Strengthening Cyber Coordination

1. Recognition of the NIST Framework by NIS Directive competent authorities
2. Empower European Network Information and Security Agency (ENISA) as convener
3. EU engagement in refining the NIST Framework
4. NIST and other U.S. participation in the EU cybersecurity Cooperation Group
5. Recognition of the NIST Framework by GDPR authorities
6. Development of transnational public-private information sharing mechanisms
7. Use of NIST Framework by EU businesses and industry groups
8. ENISA advice to European data protection institutions
9. Strengthen and broaden the EU-U.S. Cyber Dialogue

2. THE TRANSATLANTIC CYBERSECURITY COMMONS

A Shared Transatlantic Threat

"Today, unconstrained by the limits of kinetic war, by the range of missiles and bombers, by the logistics needed to support an armored division, we can succumb to digital warfare. … All democracies, not just the transatlantic ones that are joined together through NATO or the European Union, are basically under threat".

Toomas Hendrik Ilves (President, Estonia 2006-16) at the Atlantic Council on 9 February 2017

Both the EU and the United States have affirmed the need for international cooperation and harmonisation in protecting information security. The NIS Directive declares that "[g]iven the global nature of NIS problems, there is a need for closer international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues". The EU established the European Network and Information Security Agency (**ENISA**) in recognition that network and information security are "global issues" and "[t]here is a need for closer cooperation at global level to improve security standards, improve information, and promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security".[1]

Similarly in the United States, the first principle of a December 2016 report by the Commission on Enhancing National Cybersecurity, a group of high-level experts appointed by President Obama, is that "[t]he growing convergence, interconnectedness, interdependence, and global nature of cyber and physical systems means that cybersecurity must be better managed in all contexts—international, national, organizational, and individual," and their report recommended that "[t]he transnational nature of the internet makes international cooperation essential to an effective and secure digital economy".[2]

The imperatives for such cooperation apply especially to the transatlantic economy: between them, the EU and the United States make up the two largest economies in the world,accounting for 50% of global gross domestic product (GDP),[3] more than 50% of the unique IP addresses in the world,[4] and approximately one-third of global trade flows.[5] As the European Commission recognised in its recent communication, *Exchanging and Protecting Personal Data in a Globalised World,* "[t]he internet and digitization of goods and services has transformed the global economy and the transfer of data, including personal data, is part of the daily operations of European companies of all sizes, across all sectors".

The infrastructure that supports this digital economy is heavily concentrated around the North Atlantic. Figure 1 shows the global routing of internet traffic by volume.[6] It demonstrates that, of the world's 20 highest-volume hubs of internet traffic, 11 are located within the EU and five in the United States.

Figure 1 – Global Internet Map

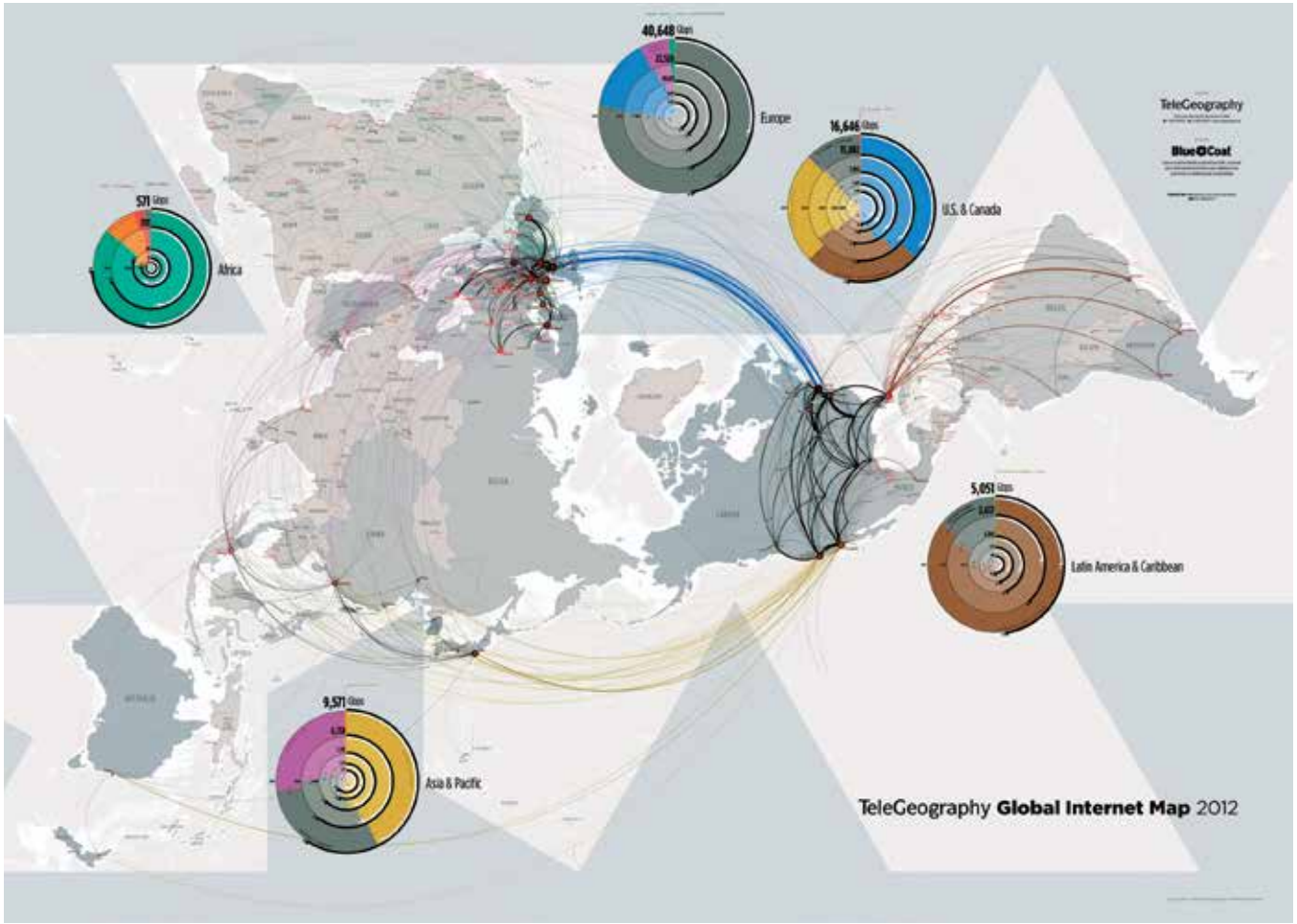


Figure 1 illustrates how thoroughly interconnected are the networks that link the United States and the EU. These networks rely on the same systems, software, and hardware, much of it supplied from outside the EU and deployed across multinational organisations and global supply chains. These networks face the same vulnerabilities and threats, the same array of technical exploits and malicious code, the same transnational cybercriminals, and the same nation-state actors. The recent theft of funds from the Central Bank of Bangladesh via the EU-based Society for Worldwide Interbank Financial Telecommunication (SWIFT) global banking network and Russian hacking during the 2016 United States election, with the prospect of similar attacks in the 2017 European elections, are stark examples of the vital interests affecting the EU and the United States jointly.

TRANSATLANTIC CYBERSECURITY

The proliferation of threats such as these to governments, individuals, and businesses large and small coming from independent actors and nation-states has increased the need for a common response.

The United States and the EU cooperate on cybersecurity and cyberdefence in a variety of forums. Under a NATO Technical Arrangement, the United States and EU exchange threat information, share best practices, and cooperate with industry partners. The United States and all EU member states are signatories to the Council of Europe Convention on Cybercrime (or Budapest Convention) and collaborate on cybersecurity in multilateral organisations, including the United Nations Group of Experts, the Organisation for Security Cooperation in Europe, Organisation for Economic Cooperation and Development, Interpol, the G7 and G20 country groups, and others. Since 2010, a joint EU-U.S. Working Group on Security and Cybercrime has conducted annual exchanges, public-private workshops, and tabletop exercises.[7]

The mounting challenge of cybersecurity across boundaries of economic sectors and national borders requires even broader and deeper cooperation. As each develops the legal frameworks, policies, and best practices described below, the EU and the United States should focus on opportunities to collaborate to harmonise laws and policies, standards and practices, and mechanisms of public-private partnerships and information sharing. As shown below, the NIST Framework provides a bridge for these purposes because it brings coherence to standards, guidelines, and practices that cross national boundaries and sectors of economies and societies.

3. TRANSATLANTIC CYBERSECURITY CONVERGENCE

As a predicate to looking at how the EU and the United States have converged in terms of cybersecurity, the report reviews significant aspects of their respective legal frameworks. It does so with a particular focus on how common aspects fit within the broader schemes of cybersecurity law and policy.

3.1 EU cybersecurity frameworks

Cybersecurity is an area of shared competence between the EU as a whole and its individual member states. Although member states have responsibility for security and law enforcement, as well as critical infrastructure such as communications and energy, the EU plays an increasing role. Cybersecurity has emerged as a top EU security priority because of the impact of cyber risks on the EU economy and the single market, as well as the attendant need for cooperation across borders. The EU's 2013 Cybersecurity Strategy propounded proposals focused on cyber resilience, network and information security and reducing cybercrime, and included the NIS Directive. In 2013 the EU also adopted a regulation renewing and expanding the mandate of ENISA as an expert body to assist in cooperation inside and outside the EU. ENISA works closely with EU member states and the private sector to "deliver advice and solutions"[8] on matters such as national cybersecurity strategies, cloud security, and the cybersecurity threat landscape.[9] The European Commission is considering a new cybersecurity strategy and a renewal of ENISA's mandate.[10]

In parallel with the NIS Directive, the EU also adopted the GDPR to create a harmonised data protection and privacy law across the EU. It expands the protection of data security and introduces data breach notification. Both the NIS Directive and the GDPR are in the process of implementation; member states have until 10 May 2018 to transpose the NIS Directive into national legislation, and the GDPR becomes applicable on 25 May 2018.

3.1.1 The NIS Directive

Under the NIS Directive, member states are required to adopt a national cybersecurity strategy that will ensure a high level of security for network and information systems if deemed "essential". It requires member states to operate national cybersecurity governance frameworks and ensure that operators of such services take "appropriate measures" to manage risks to their networks.

- **National governance frameworks.** Member states must designate competent authorities to monitor national application of the directive, and a single point of contact for cooperation across member states. The directive requires Computer Security Incident Response Teams (**CSIRTs**) to safeguard identified sectors and services by working together to monitor incidents, provide early threat warnings, respond to incidents, and cooperate with the private sector. In addition to the CSIRT network, the directive requires formation of a Cooperation Group composed of representatives from member states, the European Commission, and ENISA. This group is meant to facilitate cooperation and information exchange among member states, with ENISA providing "expertise and advice".

- **Protection of essential service networks.** The NIS Directive requires that member states identify "operators of essential services" (**OESs**) and "digital service providers" (**DSPs**) based on criteria in the directive. Member states must ensure that these entities take "appropriate and proportionate" measures to manage the risks posed to the security of their network and information systems, "having regard to the state of the art". In addition, OESs and DSPs must inform "without undue delay" the CSIRT or designated authority of any incident having a "significant" (for OESs) or "substantial" (for DSPs) impact on the service they provide. Security measures for DSPs are to take into account preventing risks; ensuring the security of systems and facilities; incident handling; business continuity management; monitoring, auditing, and testing; and compliance with international standards.

3.1.2 The GDPR data security provisions

As a regulation, the GDPR will directly apply without member states having to enact implementing legislation. Article 32 of the GDPR incorporates basic language on data security from Directive 95/46/EC that establishes an obligation to take "technical or organisational measures" to protect data security that are "appropriate to the risk" and take into account "the state of the art", "costs of implementation", and the "nature of the data" involved, but it expands this obligation in two principal ways:

- **Data security measures.** The GDPR enumerates elements that should be covered in security measures ("if appropriate").

- **Data breach notification.** Data controllers and processors are obliged to notify supervisory authorities and data subjects of certain data security incidents. Data controllers must notify (1) the applicable privacy regulators without undue delay and where possible within 72 hours, except where there are no risks to the privacy and freedoms of individuals; and (2) affected individuals when there are "high risks" to their privacy and freedoms. Data processors are required to notify data controllers "without undue delay" of all breaches.

The tasks assigned to the new European Data Protection Board in Article 70 of the GDPR include issuing "guidelines, recommendations, and best practices" for establishing data breaches and when notice is required, as well as approving codes of conduct for data security.

The GDPR and the NIS Directive represent related, roughly parallel legal frameworks. The GDPR applies basic obligations across the board, whereas the NIS Directive applies similar but potentially more specific obligations to operators of certain essential network and information services (to which the GDPR applies as well). In addition, the obligations under the NIS Directive to notify competent authorities and CSIRTs applies based on the impact on the provision of the service, not the impact on data subjects or whether there is any personal data breach (though companies covered by the NIS Directive also will have to notify data protection authorities in the event of breaches of personal data).

3.1.3 Member state cybersecurity responses

As member states transpose the NIS Directive into national law, some may introduce new laws, while others will layer the new requirements into cybersecurity laws already in place. Here, we consider responses in the United Kingdom and Germany; the first represents a horizontal approach across all sectors, while the second focuses on frameworks by sector. In addition, Italy is discussed separately in Section 3.3.4 because it has adapted the NIST Framework in its approach.

The U.K. government has confirmed it will implement the NIS Directive notwithstanding Brexit and will set out "the detailed scope and security requirements" for implementation this year.[11] In a recent public consultation, the government indicated that while it will leave open whether additional regulation might be necessary for certain sectors, it is hesitant at least for the time being to impose further regulatory requirements beyond what is required by the GDPR and NIS Directive. It emphasised "non-regulatory interventions to incentivise better cyber risk management",[12] including using breach report data to increase regulatory understanding of threats and establishing a regulators' forum. The government rejected the proposals of "specific cyber controls, risk management practices or systems testing"[13] for cyber insurance and declared that the GDPR in itself will be sufficient to catalyse significant change in cyber risk management.

The United Kingdom's implementation of the NIS Directive is intended to be consistent with the country's National Cyber Security Strategy 2016-2021, created "to support market forces to raise cyber security standards across the UK",[14] including cyber hygiene, training and skills, and legacy system upgrading. The government has already recommended certain measures to combat cybersecurity threats, notably the U.K. Cyber Essentials Scheme, developed to provide a statement of basic controls to mitigate risks from common online threats.[15] The 10 technical "Advice Sheets" that form the core of the Cyber Essentials Scheme recommend that an organisation's cybersecurity program "address risk and respond proportionately and appropriately to a level which is consistent with what risks an organisation is willing, or not, to tolerate".[16] In its focus on a risk-based approach, the Cyber Essentials Scheme is similar to the NIS Directive, GDPR, and NIST Framework. Indeed, during Prime Minister David Cameron's January 2015 visit to the United States, the two countries

agreed that they would work "with industry to promote and align our cybersecurity best practices and standards, to include the U.S. Cybersecurity Framework and the United Kingdom's Cyber Essentials Scheme".[17]

The German IT Security Act (2015) takes a sectoral approach that anticipates the requirements of the NIS Directive on critical infrastructure. It focuses on seven critical infrastructure sectors and requires operators to implement "appropriate" security measures considering "the state of the art", subject to audits every two years, and to report significant information technology-related disruptions to the Federal Office for Information Security (**BSI**).[18] The BSI takes a collaborative approach to sector-specific security standards; these are currently under development by sector-specific working groups that collaborate under the "UP KRITIS" private-public partnership scheme. The working groups include state representatives, speakers from the sector working groups in UP KRITIS, and representatives of KRITIS operators or their associations.

A German Model for Successful Public-Private Collaboration

The Alliance for Cybersecurity in Germany is a platform for cooperation between government, the private sector, and experts in science and technical bodies.[1] It now has approximately 2,000 participants. A notable success was a partnership of internet service providers and the Interior Ministry to improve network security by identifying botnet infections, notifying the infected users, and helping them clean their computers.

The United States developed a similar partnership based on this success in Germany. It resulted in a United States Anti-Bot Code of Conduct for Internet Service Providers[2] in 2012. The EU launched a similar pilot project as part of its 2013 Cybersecurity Strategy.[3]

1 National Cyber Security Alliance, https://staysafeonline.org/. (last accessed 13 April 2017)

2 Communications Security, Reliability and Interoperability Council, *U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)* (March 2012), https://www.m3aawg.org/system/files/20120322_WG7_Final_Report_for_CSRIC_III_5_0.pdf. (last accessed 13 April 2017)

3 European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (February 2013), http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf. (last accessed 13 April 2017)

3.2 United States cybersecurity regulation

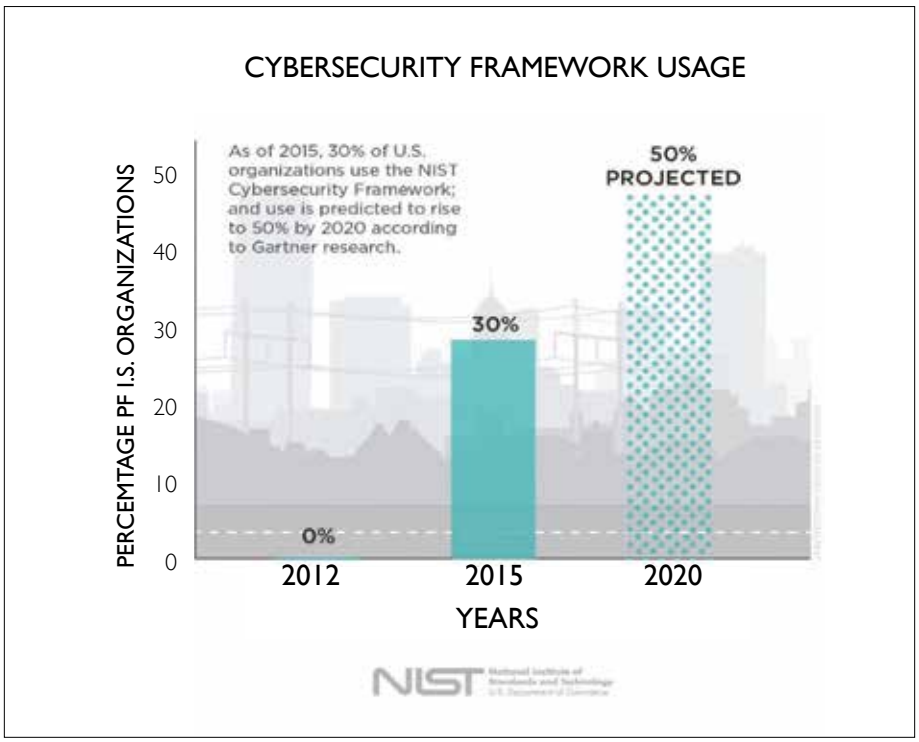
The legal framework regarding cybersecurity in the United States is a matrix of federal and state laws, regulations, and policies—some applying horizontally across sectors and others aimed at specific government or private sectors. Data breach notification like that introduced in the NIS Directive and the GDPR has been a central feature of U.S. privacy and data protection for 15 years. In addition, a widening array of federal and state agencies have taken a role in promoting cybersecurity, beginning with the Federal Trade Commission (**FTC**) and state attorneys general and expanding to include agencies that regulate securities, financial services, communications, and other sectors. These developments and ensuing enforcement proceedings and private litigation have made cybersecurity a top priority for corporate directors and managers.

Despite its well-developed cybersecurity ecosystem, with the exception of a handful of state data security laws and regulations and certain specific sectoral provisions, United States federal law does not directly prescribe data security measures. Instead, the 2014 NIST Cybersecurity Framework[19] has become the keystone of U.S. cybersecurity risk management, influencing best practices and codes of conduct, regulation, litigation, auditing, and other elements of cybersecurity in the United States.

This framework has proved to be a notable success. As shown in Figure 2 and discussed more fully in Section 3.2.2., its adoption by a wide variety of enterprises and sectoral organisations is raising the collective level of cybersecurity risk management. It is used as a benchmark by regulatory agencies, so that enforcement actions by the FTC and other agencies establish consequences when companies fail to apply appropriate practices.

The recent U.S. Commission on Enhancing Cybersecurity report recommended that the incoming administration "should build on the successes of the Cybersecurity Framework", finding that the framework "is playing an important role in strengthening risk management ecosystems" and "has tremendous value for organizations … that are resource constrained and need an efficient and effective way to address cybersecurity risk".[20]

Figure 2 – NIST Framework Usage



3.2.1 The NIST Cybersecurity Framework

The National Institute of Standards and Technology plays a vital role at the intersection of government, science and technology, and commerce—promoting innovation and competitiveness through measurement science, developing standards, and operating scientific laboratories. NIST scientists have included four winners of Nobel Prizes for science. Its role in standards development is not to prescribe standards but to act as a convener, bringing together experts from academia, the private sector, and other stakeholders to arrive at a voluntary consensus that is industry-driven. NIST's role as a technical body resembles that of ENISA, but with a remit over more than just cybersecurity.

NIST's central role in cybersecurity grew out of a 2013 executive order by President Obama that directed NIST to develop a set of "standards, methodologies, procedures, and processes" that would align with business and technology needs for cybersecurity and provide repeatable, cost-effective security measures consistent with voluntary international standards.[21] Over the following year, the first version of the framework was developed through extensive collaboration with industry, academic, and government stakeholders.[22]

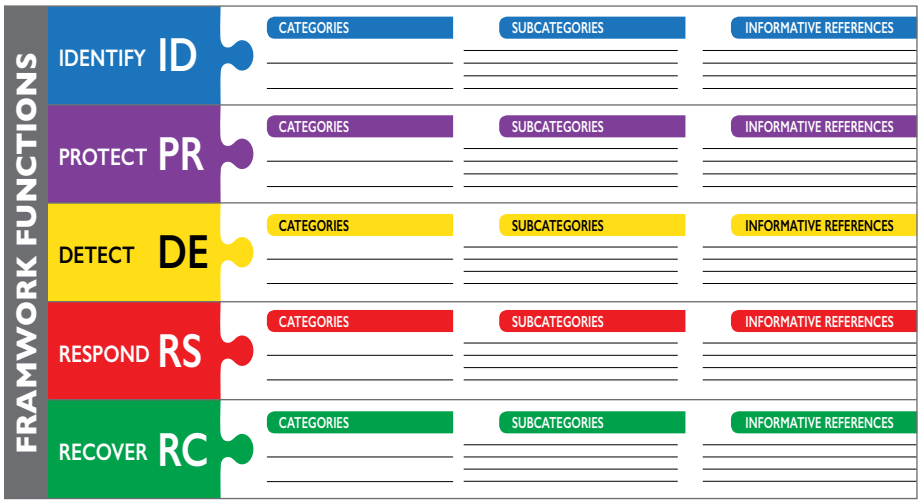
The NIST Framework avoids any set of specifications and explicitly disclaims a "one-size-fits-all" approach that could result in a tick-the-box exercise. Instead, the framework brings coherence to a wide array of existing international standards, guidelines, and practices by organising them into an analytical and organisational framework. It is designed to enable organisations to evaluate their cybersecurity programs and preparedness by assessing their risk, objectives, and processes with "a common taxonomy and mechanism". Though nominally aimed at critical infrastructure, the framework is specifically intended to be adaptable across a wide variety of organisations and sectors. It is "a living document" whose steps can be repeated "to continuously improve cybersecurity".

The NIST Framework organises these standards and recommendations into three main parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile.

- **Framework Core.** The Framework Core is a set of actions, desired outcomes, and informative references that are common across organisations and technical standards. The Core is not a checklist of actions to perform nor a single standard. Rather, it provides a conceptual framework for understanding common cybersecurity standards and practices, grouping these into four elements shown in Figure 3: functions, categories, subcategories, and informative references. These offer organisations a means of mapping their approach to appropriate cybersecurity standards and best practices.

The "functions" portion of the Framework Core categorises common cybersecurity activities at their broadest levels: identify, protect, detect, respond, and recover. The Framework Categories portion further subdivides the five functions into outcomes that are linked to an organisation's cybersecurity needs (such as asset management, access control, and detection processes). The framework "Informative References" heading incorporates specific standards into the functions and subcategories; these include leading international standards such as the ISO 27001 security management standard by the International Organisation for Standardization and International Electrotechnical Commission, the COBIT 5 framework for information technology governance and management by ISACA (formerly the International Systems Audit and Control Association), and ISA 62443 for industrial automation and control systems by the International Society for Automation.

Figure 3 – NIST Framework Core Schema



Exploring the NIST Framework

NIST maintains a resources page that includes guidance for implementing the framework in various sectors; case studies, guidelines, and tools that incorporate or map to the framework; and other reference materials on the framework: https://www.nist.gov/cyberframework/industry-resources (last accessed 13 April 2017).

- **Framework Implementation Tiers.** The Implementation Tiers give organisations better context for their cybersecurity practices and their processes in order to manage risks. Tiers characterise increasing degrees of precision and sophistication in an organisation's cybersecurity endeavours based on business requirements, and progress from "partial" (Tier 1) to "adaptive" (Tier 4). These tiers are not meant to represent maturity levels, but progressing to higher tiers is "encouraged when such a change would reduce cybersecurity risk and be cost effective".

- **Framework Profiles.** The Framework Profiles help organisations align the functions, categories, and subcategories of the Framework Core with business requirements, risk tolerances, and resources. The profiles can be used to describe the current state or the target state of specific cybersecurity initiatives. The "current profile" reflects the cybersecurity outcomes actually being achieved. The "target profile" reflects the outcomes needed to reach an organisation's cybersecurity risk management goals. By design, the NIST Framework does not prescribe profile templates, so as to enable flexibility in implementation.

Consistent with its plan to make the framework "a living document that allows for continuous improvement as technologies and threats evolve",[23] on 10 January 2017 NIST released a draft version 1.1 for public comment. This version adds guidance on cybersecurity metrics and supply chain risk management issues reflecting stakeholder feedback on the prior version. NIST has requested and received comments with an eye towards a workshop late in 2017.

3.2.2 Widespread use of the NIST Framework

The NIST Framework has proved itself through broad use by the business community. As shown in Figure 2, it is employed by 30% of companies in the United States, projected to reach 50% by 2020, thereby increasing protection of the cybersecurity commons. Among the sectoral associations that that have incorporated the framework into cybersecurity recommendations are auto manufacturers, the chemical industry, the gas industry, hotels, water works, communications, electrical distribution, financial services, mutual funds, restaurants, manufacturing, retail sales, transportation, and corporate directors.

Regulatory agencies have taken note of the NIST Framework's importance. In particular, the Securities and Exchange Commission, which regulates the securities market, has acknowledged that the NIST Framework should be actively considered as a benchmark by boards of directors when evaluating their cyber risk management policies.[24] In addition, the FTC, which has broad jurisdiction over consumer protection, has made clear that implementation of the NIST Framework will be regarded as a best practice in determining unfair data security practices.[25] The Department of Homeland Security and Department of Energy have each adopted policies to encourage use of the NIST Framework by critical infrastructure owners and operators, as well as in the energy sector.[26, 27]

Notably, adopters of the NIST Framework have included international organisations. ISACA, which develops the COBIT 5 information security framework, has produced a cybersecurity program based on the NIST Framework "that can provide enterprise leaders confidence in the effectiveness of their organization's cyber security governance, processes, and controls".[28] The Investment Industry Regulatory Organization of Canada lists the framework as a "foundational reference" for its best practice guide for securities dealers in that country.[29] As discussed in Section 3.3.4, Italy has incorporated the NIST Framework into its national cybersecurity framework.

3.2.3 Data breach notification and information sharing

As mentioned above, breach notification plays a central role in U.S. privacy and data protection, with nearly every state and the District of Columbia adopting laws requiring notification of regulators or customers.[30] While the specifics of these vary, as a general matter they require notice without unreasonable delay to customers of a breach that presents some risk of harm to the customer, and many require some broader or earlier notice to regulators.

Recent legislation and a series of presidential orders have sought to encourage information sharing concerning cybersecurity threats and incidents among the private sector and with the federal government. A 1998 executive order encouraged critical infrastructure owners and operators to collaborate in identifying threats, best practices, and mitigation through trusted entities referred to as Information Sharing and Analysis Centres (**ISACs**).[31] In 2015, President Obama expanded this to encourage private sector entities that were unable to join ISACs to share information through Information Sharing and Analysis Organizations (**ISAOs**).[32] The same executive order that led to the NIST Framework directed federal government agencies to provide "classified cyber threat and technical information" to certain critical infrastructure businesses.[33]

Congress has supported these approaches and, in 2015, passed the Cybersecurity Information Sharing Act (**CISA**),[34] which takes additional steps to encourage information sharing and establish requirements for the protection of personal data contained in information that is shared. The act provides legal authority for private entities to monitor and defend their networks against cybersecurity threats and share threat information with other private entities and the federal government. In exchange for companies reporting cyber threat indicators and defensive measures to local and federal governments and for other private monitoring and reporting networks, CISA provides safe harbours including liability protection.

CISA also charges federal agencies with stepping up the sharing of cybersecurity threat information, including procedures and a digital portal with private entities, non-federal government agencies, and the general public. This increased public-private partnership in cybersecurity has altered the mindset of agencies: the Department of Justice, Department of Homeland Security, FTC, and state attorneys general have recognised that cybersecurity attacks are so pervasive

that government regulators and prosecutors should treat organisations attacked as victims in most instances and move away from treating them as targets for legal action. In these respects, CISA shares significant similarities with the objectives of the NIS Directive, which seeks to also enhance breach reporting on a mandatory or voluntary basis.

Table 1 – Key points in common Between NIST Framework, the NIS Directive, and GDPR

Touchpoint	NIST Framework	GDPR	NIS Directive
Adoption by organisations of risk-based cybersecurity measures (Section 3.3.1)	Organisations to use the framework based on their own risk assessment of framework itself disclaims a "*one-size-fits-all*" approach for organisations.	Organisations must adopt a "*level of security appropriate to the risk*" and consider the "*costs of implementation*" in determining what security would be appropriate.	Organisations are to adopt security measures that are "*appropriate and proportionate … to manage the risks posed to the security of network and information systems*" that they use.
Voluntary, consensus-based public-private standards development (Section 3.3.2)	Framework is technology neutral and industry neutral and created through collaborative stakeholder input from the government and the private sector, including as regards updated version 1.1.	Contains standards—not prescriptive rules—regarding how organisations can demonstrate compliance, including through industry-led "*approved codes of conduct*".	Expresses a preference for standards that are voluntary, market driven, technology neutral, and industry neutral; does not prescribe how an organisation can demonstrate compliance.
Adaptable approach that reflects rapid changes (Section 3.3.3)	Organisations using the NIST Framwork may progress to higher tiers; in addition, the framework itself is regarded as a "*living document*" that will be continually updated.	Organisations are to ensure that security measures are "*state of the art*".	Organisations are to ensure that security measures are "*state of the art*".
Promotion of information sharing (Section 3.3.4)	CISA and executive orders encourage voluntary sharing of cyber threat information by providing liability protection and facilitating trusted information-sharing organisations.	Requires timely breach notification obligations if sufficient level of risks for individuals.	Network and information service providers must notify competent authority of certain breaches and are encouraged to share threat information. Notifying party is not subject to additional liability as a result of notification.
Harmonised international language for stakeholder communication (Section 3.3.5)	Framework creates an international taxonomy and cyber risk language grounded in consensus, best practices, and international standards.	ENISA, with respect to EU cybersecurity generally, has recommended creating a "*common understanding of concepts and terminology*".	Acknowledges the need for a global approach and "*closer international cooperation to improve security standards*" and "*promote a common global approach*" to cybersecurity.

3.3 Transatlantic cybersecurity convergence

Although the GDPR and NIS Directive differ in process from the NIST Framework by empowering authorities to prescribe data security measures, they give authorities latitude as to what such requirements should be and how they are arrived at. On close examination, both the NIS Directive and GDPR have key points in common with the NIST Framework summarised in the table and discussion that follows. These touchpoints provide a sound basis for EU institutions—the European Commission, ENISA and member states and their competent authorities and data protection authorities—to bring the NIST Framework into their implementation of the NIS Directive and GDPR as outlined in Section 4.

3.3.1 Risk-based security measures

The United States and EU cybersecurity frameworks converge around risk assessment as the touchstone of effective cybersecurity. The NIS Directive calls for "[a] culture of risk management involving risk assessment and the implementation of security measures appropriate to the risks faced". Cybersecurity measures should be "proportionate to the risk presented by the network or information system concerned", and member states should ensure that OESs take technical and organisational measures that are "appropriate and proportionate … to manage the risks posed to the security of network and information systems which they use in their operations". While member states may specify what such "appropriate and proportional" measures may entail, the NIS Directive itself is non-prescriptive.

Article 32 of the GDPR contains similar language: taking into account various listed factors, the outcome it demands is "a level of security appropriate to the risk". Similarly, while the GDPR mandates breach notification, this obligation is risk-based; only breaches that may be a "risk" to individuals will need to be brought to the attention of regulators and only those that are "high risk" will need to be brought to the attention of individuals.

Assessment of information risk and measures tailored to risk is at the centre of the NIST Framework. It builds on risk assessment processes, is designed to integrate with existing risk management, and aims "to provide a flexible and risk-based implementation that can be used in a variety of cybersecurity risk management processes".

The NIST Framework thus provides a tool by which authorities or businesses can conduct the risk assessment that is necessary under the NIS Directive and the GDPR and thereby evaluate what are "appropriate measures". Indeed, the "protect" Core function of the NIST Framework refers to developing and implementing "appropriate safeguards" to protect delivery of services. In addition, a key feature of the NIST Framework is to enable businesses to adopt measures reflecting their assessment of the cyber risk for their business and their own posture towards such risks. If a breach occurs, a business that has adopted the NIST Framework may be in a better position to determine whether risk thresholds that trigger notice to supervisory authorities or data subjects have been reached.

A corollary to the focus of a risk-based approach is that measures should be cost effective. The NIS Directive expressly acknowledges that cybersecurity measures should "avoid imposing a disproportionate financial and administrative burden". The GDPR provides that data security measures should take into account among other things "the costs of implementation". The NIST Framework "identify" Core function seeks to "manage cybersecurity risk to systems, assets, data, capabilities," which requires understanding among other things, "business context … resources … and business needs", and identifies as a management function decisions about risk appetite and budget. It refers to selection of measures and references "that are cost-effective and efficient" in enabling organisations to manage their cybersecurity risk.

Siemens and the NIST Framework

As a leading global supplier of systems for power generation and transmission as well as computer systems, Siemens AG is deeply involved in critical infrastructure sectors throughout the world. Incorporated in Germany, it has subsidiaries in the United States and across the EU.

Siemens is one of several international companies to participate actively in consultations on the NIST Framework. In 2016 comments, Siemens Industry Inc. submitted that "*the entire document provides useful information to an audience of wide experience levels in the area of cybersecurity*", and called for private sector involvement "*in providing input directly to the Framework … and to the international standards bodies that support the implementation of the cybersecurity activities that the Framework describes*".[1]

Siemens produced a May 2015 white paper for the United Kingdom Institution of Engineering & Technology laying out steps to improve resilience in the energy industry that are based on the NIST Framework. The paper states that "use of frameworks is essential in many areas of engineering" and focuses on the NIST Framework as "*a simple yet powerful framework which helps those responsible for critical infrastructure shape their thinking and help to improve the resilience of their operation*".[2]

---

1 Siemens, *Views on the Framework for Improving Critical Infrastructure Cybersecurity* (February 2016) http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160208_Siemens.pdf (accessed 13 April 2017).

2 Siemens, *Cybersecurity in the Energy Industry* (May 2015), at page 11, https://www.downloads.siemens.com/download-center/download?DLA20_104 (accessed 13 April 2017).

3.3.2 Voluntary, consensus-based public-private standards development

The NIS Directive encourages "[s]tandardisation of security requirements" as "a market-driven process" and incorporates by reference Regulation EU No 1025/2012 on European standardisation (the Standards Regulation).[35] In turn, the directive expresses a preference for standards that "are voluntary and should be market-driven, whereby the needs of the economic operators and stakeholders directly or indirectly affected by such standards prevail, and should take into account the public interest and be based on the founding principles, including consensus". The NIS Directive also recommends that national standards be technology neutral and industry neutral, while allowing industry-specific customisations by industry groups (e.g., the EU's Cloud Select Industry Group). For example, the NIS Directive requires that, with respect to digital service providers, any security requirements proposed by member states consider, among other things, "compliance with international standards". In turn, ENISA's 2016 *National Cyber Security Strategy Good Practice Guide* calls for establishing public-private partnerships "to pool the expertise of the private and public sector".[36]

Similarly, United States law and policy reflects a parallel commitment to voluntary, technology-neutral, industry-neutral, and industry-driven standards by both statute and regulation.[37] The NIST Framework embodies this approach. It was created through a series of highly collaborative workshops and stakeholder input that involved the government, the private sector, and other stakeholders. This collaboration continues as NIST considers input from stakeholders on its draft version 1.1 of the framework.

As NIST's revision process moves forward, there is an opportunity for transatlantic cooperation in a risk-based and standards-based approach to cybersecurity that will strengthen global networks and encourage voluntary industry practices. The NIST Framework incorporates a range of international standards referred to above. Engagement of EU stakeholders, including EU bodies and standards development organisations, will ensure all applicable international stakeholders are included and a framework is developed that is even more adaptable to implementation of EU cybersecurity laws.

Ernst & Young's Global Use of the NIST Framework

Ernst & Young (EY), headquartered in London, is one of the world's largest professional services firms and a "Big Four" accounting firm. EY uses the NIST Framework for both its own security measures and those of its clients.

According to EY, the most useful portion of the NIST Framework is the "[Framework] *Core's common language/risk management approach*". This has allowed the firm "*to implement standard processes throughout EY's global offices*", and assist clients in doing the same. In EY's experience, "*the Framework aligns with business objectives by building flexible, repeatable processes and procedures to identify, assess, and manage cyber risk*".[1]

1 Ernst & Young, *National Institute of Standards and Technology, Cybersecurity Framework, Request for Information* (February 2016), at page 3 https://www.nist.gov/sites/default/files/documents/2017/02/14/20160222_ernst_young.pdf (accessed 13 April 2017).

The NIS Directive requires OESs to provide "evidence of the effective implementation of security policies". The GDPR similarly requires that businesses be able to demonstrate they are complying with their security obligations—without prescribing rules on how this demonstration should occur. Instead the GDPR sets out standards that satisfy these so-called accountability obligations such as "privacy by design" and "privacy by default" mechanisms, as well as other measures such as "approved codes of conduct".[38] A business that intends to demonstrate that it has satisfied the GDPR's "privacy by design" standard could do so through the NIST Framework. For example, the Framework Implementation Tiers and Framework Profiles, if appropriately used, will allow a business to demonstrate that data security considerations are integrally incorporated into its businesses processes, rather than an afterthought. A business also could demonstrate that its security measures are constantly evolving and adaptive in response to the framework tiers and profiles.

The NIST Framework in Asia and Beyond

Nippon Telegraph and Telephone Corporation (NTT) is one of the world's leading telecommunications providers. While headquartered in Japan, NTT has subsidiaries across the world, including in the EU and the United States and is listed on stock exchanges in Tokyo, New York, and London.

NTT has used the NIST Framework, declaring that it is "*very powerful and has benefits beyond its original design purpose. NTT has used it on multiple occasions, in particular for capability assessment and mapping purposes. These occasions cover both internal NTT applications as well as with other Japanese companies from multiple sectors. We have also used it in our publication to communicate to C-suites on cyber security risk management in a holistic manner. At all of these instances, we have found the Framework functions to be very effective as a common language for people with different backgrounds.*"[1] NTT provided five case studies where it found the NIST Framework to be particularly useful.

1 Nippon Telegraph and Telephone Corporation, Views on the *Framework for Improving Critical Infrastructure Cybersecurity* (February 2016), http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160201_NTT.pdf

If EU regulators, such as the Article 29 Working Party and its successor, the European Data Protection Board, were to interpret "accountability" measures and "approved code of conduct" to encompass the NIST Framework (steps that would be facilitated by accountability language proposed for version 1.1), that would demonstrably allow businesses to rely on their adoption of the NIST Framework to also meet their accountability obligations under the GDPR. Similarly, ENISA, as it did in its *NCSS Good Practice Guide*, could import additional thinking from the NIST Framework into its recommended best practices.

3.3.3 An adaptable approach to keeping up with rapid change

One of the challenges of cybersecurity is the rapid pace of change in technology and the evolving threats. As the European Commission put it in its 2013 Cybersecurity Strategy, "cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom". To keep up, cybersecurity laws and policies cannot remain static, but must be nimble and adaptable to rapid changes.

Hence both the NIS Directive and GDPR Article 32 direct that security measures should take into account "the state of the art". The NIST Framework addresses this challenge in several ways: by encouraging progression to higher Implementation Tiers that reflect "an increasing degree of rigor and sophistication in risk management", by recommending repeating use of the framework "to continuously improve cybersecurity", and by making the framework "a living document" that "will continue to be updated and improved". The NIST Framework thus provides a set of tools for establishing the state of the art and anticipates changes in practices and in the framework as the state of the art changes.

3.3.4 Promotion of information sharing

Sharing of information about cyber threats or incidents—whether by providers giving notification to relevant authorities, entities cooperating with each other, or relevant authorities sharing with each other through a cooperation group or ENISA—has been a growing element of national cybersecurity policies. Data breach notification to public authorities is one form of information sharing. While the NIS Directive (like the GDPR) contains mandatory breach notification obligations, it also recognises the tensions between the public and private interests in disclosing breaches:

> Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats against possible reputational and commercial damage for [OESs and DSPs] reporting incidents.[39]

In particular, in seeking to balance these interests the NIS Directive provides that "[n]otification shall not make the notifying party subject to increased liability" with respect to both OESs and DSPs. Similarly in the United States, mechanisms for sharing information have been a major element of legislation and policy, in particular, in CISA to enhance sharing of information about cybersecurity threats.

CISA allows private sector entities to monitor networks and share cyber threat information (provided certain personal information has been removed). There are comparable mechanisms for information sharing in the EU. For example, the U.K. National Cyber Security Centre established the Cyber-security Information Sharing Partnership, a joint industry and government initiative to enable real-time sharing and increase situational awareness.[40] Since effective sharing of information concerning risks is an important goal on both sides of the Atlantic, it makes sense to explore increased avenues of information sharing on a transnational basis.

The Italian National Cybersecurity Framework

Italy has adopted Il Framework Nazionale di Cyber Security (the Italian Framework), developed by the Cyber Security National Lab, in collaboration with the private sector and academia. It is substantially modelled on the NIST Framework, with its emphasis on critical infrastructure protection, international harmonisation, public-private cooperation, and adaptability. The Italian Framework, its authors say, is aimed at creating a common language to compare business practices to mitigate cybersecurity risks. "*The choice to use the US Framework is based on the idea that the answer to cyber threats should provide an alignment at [an] international level, not only at [a] national level*".[1]

The Italian model is worthy of study because it is built on principles that should be common to any domestic or global cybersecurity initiative. It shapes the application of the Italian Framework to key sensitive critical infrastructure sectors in Italy and Italian privacy law.

1 CIS Sapienza, *Italian Cybersecurity Report: A National Cyber Security Framework version 1.0* (2015) (English translation, February 2016), at page 2, http://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf (last accessed 13 April 2017).

3.3.5 A harmonised international language for stakeholder communication

The NIS Directive acknowledges the current "[l]ack of common requirements" in the EU that has resulted in an "unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union", which in turn need to be addressed through "a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information, cooperation and common security requirements".

While the directive aims to improve the EU's overall cybersecurity capabilities by enhancing cooperation among member states, it also declares that "[g]iven the global nature of NIS problems, there is a need for closer international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues".

ENISA too has emphasised the need for international cooperation.[41] Specifically, ENISA has recommended creating a "common understanding of concepts and terminology"[42] with respect to cybersecurity communications. In recommending that a public-private partnership be adopted where private companies own critical infrastructure, ENISA appears to endorse the structure of the NIST Framework Core. In this context, ENISA describes "objectives" for such a partnership, which appear to mirror with the Framework Core by referring to "deterring", "protecting", "detecting", "responding", and "recovering" in relation to cybersecurity events.[43] In addition, the NIST Framework's common language is grounded in consensus, best practices, and international standards, better equipping organisations to discuss risk management and cybersecurity both internally (e.g., with company executives and boards) and externally (e.g., with business partners and suppliers) across their ecosystems.

Forging a United Response to Universal Threats

The key elements of the NIS Directive, GDPR, and NIST Framework—a focus on risk assessment and risk management; emphasis on the use of broadly applicable, consensus-based standards; cooperation among government, the private sector, and other stakeholders; increased sharing of information about threats, incidents, and security practices; and a unifying approach—provide fertile ground for greater transatlantic cooperation on cybersecurity.

The NIST Framework—as a voluntary, risk-based taxonomy of standards and practices set out using common cyber-risk-management language that is not specific to any industry or country and was developed with strong public and private sector input—provides a blueprint on which government, businesses, and other stakeholders can build strong cybersecurity on both sides of the Atlantic.

4. A PATH TO INCREASED TRANSATLANTIC CONVERGENCE AND COOPERATION

4.1 The NIST Framework as a European cybersecurity framework

The widespread adoption of the NIST Framework not only across a range of government bodies and business sectors in the United States but also by governments and business in Europe is a result of the framework's success in practice. The success of the NIST Framework lies in its comprehensiveness and its adaptability to different kinds of risks, organisations, and standards or practices. This same adaptability and comprehensiveness can make it a valuable tool in the implementation of the NIS Directive and GDPR governance that will enhance the coherence of cybersecurity programs in the EU. EU member states may wish to converge their cybersecurity programs towards the NIST Framework as a lodestar for security and resilience.

The NIST Framework is easily adaptable to key elements of the NIS Directive and the GDPR.

As shown in the preceding section, the NIST Framework harmonises with requirements under the NIS Directive and the GDPR. It provides a toolkit for organisations to adopt security measures that are (1) appropriate to the level of risk, (2) cost-effective, and (3) state of the art. Because the NIST Framework incorporates a suite of informative references to leading cybersecurity standards and will be updated continuously to reflect feedback and changing standards, it reflects the state of the art.

The NIST Framework also embodies the consensus, private-sector-driven approach to standards development that—on both sides of the Atlantic—is enshrined in law and important to technology development. Employing this collaborative, multistakeholder approach in the implementation of the NIS Directive and the GDPR will reinforce the sharing of information that is another element of these two measures and is necessary to effective cybersecurity protection.

Forging a United Response to Universal Threats

A common cybersecurity framework can bring the power of network effects to transatlantic cybersecurity protection.

As discussed above and as recognised by the European Commission, ENISA, and other government bodies in the EU, the transnational nature of the internet and cybersecurity threats requires transnational solutions. It is imperative that the EU and the United States speak the same language in terms of understanding each other's cybersecurity postures and responding to the global threats. As the Italian Framework illustrates, the NIST Framework can provide a cohesive language worldwide.

Getting organisations to adopt effective security measures is essential to strengthening cybersecurity in general. This goal is central to the NIS Directive and to the European Commission and national cybersecurity policies, as well as being an important principle of the GDPR. Wider adoption of the NIST Framework could increase understanding and uptake of cybersecurity measures based on widely accepted international standards. On the other hand, if businesses or industries have to adopt a unique cybersecurity framework for each European market in which they operate, they may choose, on cost and organisational grounds, to defer or to adopt suboptimal cybersecurity compliance for their EU-based operations. This could deteriorate the quality of cybersecurity across the EU.

As Germany's BSI states:

> Due to the globality of the market, IT security standards and IT security certifications are only relevant for guaranteeing the trustworthiness of hardware and software products when based on international standards such as 'Common Criteria.' Large companies operating internationally are only prepared to invest in testing with subsequent certification on the basis of international standards.[44]

Thus, national or regional standards will work against adoption in practice. By contrast, a unified approach can produce "network effects"—thereby strengthening cybersecurity across the EU and throughout the transatlantic cybersecurity commons. If EU authorities apply the NIST Framework, this would encourage multinational businesses to deploy robust and cost-effective cybersecurity measures for their EU operations more rapidly.

TRANSATLANTIC CYBERSECURITY

Because the NIST Framework is an overarching framework that unifies a variety of international cybersecurity standards and is technology and standards neutral, adoption would have the benefit of avoiding reliance on a single standard. This avoids the risk of "capture" by any particular standards development body as well as suboptimal uptake. In addition, both the EU and United States are seeking to aid development of a cybersecurity ecosystem: technologies, industry, standards, human skills, and other conditions that can foster better cybersecurity (major goals of the EU Digital Single Market strategy). Applying the NIST Framework widely in EU implementation of the NIS Directive and the GDPR would enable cybersecurity technology providers incubated within the EU to compete better internationally and create cybersecurity products and services that are relevant not only within the EU but for the United States and other international markets as well.

4.2 Ways to make the NIST Framework a European cybersecurity framework

1. **Recognition of the NIST Framework by NIS Directive competent authorities**
   During the implementation of the NIS Directive, individual member states, competent authorities, and the Cooperation Group should recognise the NIST Framework as an "appropriate and proportionate technical and organisational [security] measure" with respect to security obligations of OESs and DSPs. The Italian Framework illustrates how this recognition may occur.

2. **ENISA as EU convener**
   Consistent with its current mandate, and reinforced in new legislation, ENISA—in conjunction with the NIS coordinating group—should play a role parallel to NIST by (1) convening stakeholders on cybersecurity standards and best practices and (2) engaging with international standards-development organisations on cybersecurity standards. Many member states are presently considering national cybersecurity strategies and governance frameworks in connection with their implementation of the NIS Directive, and ENISA is actively advising on these matters. By acting as a convener of stakeholders, ENISA could assist member states in bringing a broad array of stakeholders into the discussion, considering the NIST Framework as an appropriate measure, and further aligning security standards with each other and the United States.

3. **EU engagement in refining the NIST Framework**
   EU stakeholders (especially ENISA, the European Commission, member states, and EU businesses) should engage actively with NIST in refining the NIST Framework. Version 1.1, an update to the earlier version, was released for public comment on 10 January 2017. Engagement by EU stakeholders in NIST's ongoing process could to help tailor the NIST Framework as an international cybersecurity tool that also reflects additional EU-appropriate elements.

4. **NIST and other United States participation in the EU cybersecurity Cooperation Group**
   The Commission should bring the U.S. Department of Commerce, including NIST, and the U.S. Department of Homeland Security into the Cooperation Group pursuant to Article 13 of the NIS Directive. This would help to enhance sharing of information on threats and best practices and broaden the relevance of the Cooperation Group's work.

TRANSATLANTIC CYBERSECURITY

5. **Recognition of the NIST Framework by GDPR authorities**
   As with the NIS Directive, individual member state data protection authorities and the Article 29 Working Party/European Data Protection Board, in coordination with ENISA, should recognise application of the NIST Framework as an "appropriate technical and organisational measure". Similarly, the Article 29 Working Party/European Data Protection Board should recognise the NIST Framework as an "approved code of conduct" for accountability under Article 32 (3) of the GDPR and other GDPR obligations.

6. **Development of transnational ISACs and ISAOs**
   The EU Commission, member states, plus ENISA or transnational institutions may wish to collaborate with the United States government to create and operate transnational information sharing and analysis organisations (similar to ISAOs) and information sharing and analysis centres (similar to ISACs). The use of a common taxonomy and risk-based language—such as the NIST Framework—as part of this process will be essential.

7. **Use by EU businesses and industry groups**
   Adoption of the NIST Framework by businesses (such as Siemens) and industry groups (through, for example, codes of conduct and best practice recommendations) could further spur "network effects" in the adoption of the framework.

8. **ENISA advice to European data protections institutions**
   To enhance coordination on cybersecurity measures to implement the GDPR data security provisions, ENISA should advise the European Data Protection Supervisor and the European Data Protection Board established under the GDPR.

9. **Strengthen and broaden the EU-US cybersecurity dialogue**
   In view of the issues of implementation faced under the NIS Directive and the GDPR, the existing EU-U.S. Cybersecurity Dialogue should broaden its focus to include discussion of harmonising frameworks and participation of the Article 29 Working Party, ENISA, and a broad cross-section of civil society and private sector stakeholders.

REFERENCES

1 Recital 19, Regulation (EC) 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. This regulation has been repealed by Regulation (EU) 526/2013 of 21 May 2013.

2 Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* (1 December 2016), at pages 4 and 47, https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf (accessed 13 April 2017).

3 Joshua Meltzer *The Importance of the Internet and Transatlantic Data Flows*, Global Economy and Development Paper 49 (October 2014), at page 4, https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf (accessed 13 April 2017).

4 Country IP Blocks, *Allocation of IP addresses by country*, https://www.countryipblocks.net/allocation-of-ip-addresses-by-country.php (accessed 14 April 2017).

5 Eurostat, *USA-EU-international trade and investment statistics* (February 2015), http://ec.europa.eu/eurostat/statistics-explained/index.php/USA-EU_-_international_trade_and_investment_statistics. (accessed 13 April 2017)

6 Telegeography, *Global Internet Map*, https://www.telegeography.com/telecom-maps/global-internet-map.html (accessed 12 April 2017).

7 European Union – External Action, *Fact Sheet: EU-US cooperation on cyber security and cyberspace*, (26 March 2014) http://eeas.europa.eu/archives/docs/statements/docs/2014/140326_01_en.pdf (accessed 13 April 2017).

8 *About ENISA*, https://www.enisa.europa.eu/about-enisa (accessed 20 February 2017).

9 *Id.*

10 European Commission, *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry* (5 July 2016), at page 5, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0410&from=EN (accessed 13 April 2017).

11 HM Government, *Cyber Security Regulation and Incentives Review* (December 2016), at page 12, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf (accessed 27 January 2017).

12 *Id.* at page 3.

13 *Id.* at page 19.

14 *Id.* at page 10.

15 HM Government, *Cyber Essentials Scheme Summary* (June 2014), at page 3, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf (accessed 27 January 2017).

16 UK National Cyber Security Centre, *10 Steps: Risk Management Regime* (16 February 2017), https://www.ncsc.gov.uk/guidance/10-steps-information-risk-management-regime (16https://www.ncsc.gov.uk/guidance/10-steps-information-risk-management-regime (accessed 13 April 2017).

17 The White House, *Fact Sheet: U.S.-United Kingdom Cybersecurity Cooperation* (16 January 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation (accessed 13 April 2017).

18 Federal Office for Information Security (BSI), *The State of IT Security in Germany* (October 2016), at page 48, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2016.pdf?__blob=publicationFile&v=3 (accessed 13 April 2017).

19 NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, 12 February 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (accessed 14 April 2017)

20 Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* (1 December, 2016), at page 19, https://obamawhitehouse.archives.gov/sites/default/files/docs/cybersecurity_report.pdf (accessed 13 April 2017).

21 Exec. Order No. 13636, 78 Fed. Reg. 11737 at page 11741 (19 February 2013). See also *id* at pages 3-11.

22 NIST, *Cybersecurity Framework FAQS Framework Basics*, https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics (accessed 23 January 2017).

23 Undersecretary Patrick J. Gallagher in NIST Press Release, "NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments" (22 October 2013), https://www.nist.gov/speech-testimony/press-briefing-preliminary-cybersecurity-framework (accessed 13 April 2017).

24 See, e.g., Commissioner Luis Aguilar, *Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus*, https://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.VNpDDPnF8Ro (accessed 20 February 2017).

25 Federal Trade Commission, *The NIST Cybersecurity Framework and the FTC*, https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc (accessed 20 February 2017).

26 United States Department of Homeland Security, *Using the Cybersecurity Framework*, https://www.dhs.gov/using-cybersecurity-framework (accessed 20 February 2017).

27 United States Department of Energy, *Reducing Cyber Risk to Critical Infrastructure: NIST Framework*, https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/reducing-cyber-risk-critical-infrastructure-nist (accessed 20 February 2017).

28 Press Release, *ISACA Produces New Audit Program Based on NIST Framework* (10 January 2017), https://www.isaca.org/About-ISACA/Press-room/News-Releases/2017/Pages/ISACA-Produces-New-Audit-Program-Based-on-NIST-Framework.aspx (accessed 13 April 2017).

29 Investment Industry Regulatory Organization of Canada, *Cybersecurity Best Practices Guide – For IIROC Dealer Members,* at page 10, http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf (accessed 13 April 2017).

30 E. McNicholas and V. Mohan (eds.), *Cybersecurity: A Practical Guide to the Law of Cyber Risk* (2015) (Practicing Law Institute), at page 2-5.

31 White House, *Critical Infrastructure Protection*¸ Presidential Decision Directive NSC-63 (22 May 1998), https://fas.org/irp/offdocs/pdd/pdd-63.htm (accessed 14 April 2017).

32 White House, Promoting Private Sector Cybersecurity Information Sharing, Executive Order 13691 (12 February 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf (accessed 14 April 2017).

33 Section 4(c) of Exec. Order No. 13636, 78 Fed. Reg. 11737 (19 February 2013) https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (accessed 14 April 2017).

34 Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113 (18 December 2015).

35 Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC, and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1025&from=en (accessed 12 December 2016).

36 ENISA, *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies* (November 2016), https://www.enisa.europa.eu/publications/ncss-good-practice-guide (accessed 13 April 2017).

37 National Technology Transfer and Advancement Act, 15 U.S.C. § 372; Office of Management & Budget Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities* (revised 27 January 2017).

38 Article 24(3) and Recital 78, GDPR.

39 Recital 59, NIS Directive.

40 National Cyber Security Centre, *Cyber-security Information Sharing Partnership (CiSP)*, https://www.ncsc.gov.uk/cisp (accessed 13 April 2017).

41 ENISA, *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies* (November 2016), at page 53 (Recommendation 4).https://www.enisa.europa.eu/publications/ncss-good-practice-guide (accessed 13 April 2017).

42 *Id*. at page 53 (Recommendation 5).

43 *Id*. at page 35 (paragraph 4.11).

44 Federal Office for Information Security (BSI), *The State of IT Security in Germany* (October 2016), at page 54, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2016.pdf?__blob=publicationFile&v=3 (accessed 13 April 2017).

U.S. CHAMBER OF COMMERCE

1615 H Street, NW | Washington, DC 20062
uschamber.com