A SECURITY SYMPHONY

HARMONIZING CYBERSECURITY REGULATION

Global Cybersecurity Group | ASPEN DIGITAL

aspen institute

TABLE OF CONTENTS

INTRODUCTION

The global cybersecurity regulatory environment is deeply fragmented, inefficient, and often ineffective. This is costly on many levels—within and across nations. Paradoxically, regulatory disharmony can prevent the very outcomes that policymakers intend. It is frequently a key factor preventing the actions that could meaningfully reduce malicious cyber activity and the harm it causes at scale: information sharing at machine speed ; security innovations; processes and technology; transparency and consistency in liability; and resilience. Against this backdrop it should come as no surprise that myriad public and private sector organizations and, increasingly, community groups, have called for a common, baseline approach to cybersecurity regulation.

Progress with harmonizing cybersecurity regulation (and close cousins privacy and safety regulations[2] [3]) has been a decades-long pursuit and frustratingly slow. Most nations now have some form of cybersecurity or related regulation, often informed by strategy or policy, a significant shift from a decade ago. Myriad other global and regional multi-nations governance committees and working groups have attempted to achieve at least a foundational set of principles on which nations can build a measurable and effective set of regulatory interoperations.

These efforts have brought incremental progress, including:

- The Council of Europe Convention on Cybercrime (the Budapest Convention);
- The United Nations Group of Governmental Experts on advancing responsible State behavior in cyberspace;
- The United Nations permanent and ad hoc committees on cybersecurity including that which resulted in the adoption of a cybercrime treaty;

[1] "Automated Indicator Sharing (AIS) | CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais.

[2] Australia eSafety Commissioner. "Learn about the Online Safety Act | *ESafety Commissioner.*" ESafety Commissioner, 2022, www.esafety.gov.au/newsroom/whats-on/online-safety-act.

[3] "Cyber Resilience Act | Shaping Europe's Digital Future." *Digital-Strategy.ec.europa.eu*, digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

- The World Economic Forum's (WEF) work on cybersecurity regulation through its Center for Cybersecurity; and
- The Tallinn Manuel and its versions.

A wide range of industry- and academic-led work in this arena has also sought to influence global frameworks and create uptake for change. This includes internationally inclusive non-profits including the WEF's Cybercrime Atlas project, the US-originated network of sector-specific cybersecurity Information Sharing and Analysis Centers and Information Sharing and Analysis Organizations and the Global Forum on Cyber Expertise.

Yet, harmonization of cybersecurity regulation remains elusive.

Curiously, regulatory harmonization, and the policies that inform its development, lags behind increasingly harmonized operational practices in singular and collective defense against malicious cyber-physical activity. The amplification and intensity of the cyber threat environment has prompted the industry and governmental sharing of tactics, techniques and procedures together with collaborative research into interception, interdiction and disruption of digital activity with harmful intent and/or effect.

The absence of a sophisticated, responsive globally harmonized regulatory environment causes friction across the many dimensions: legal and legislative, risk and business, research and development, innovative and technological, strategy and workforce.

Multi-national adoption of technical standards and guidance (including the ISO/IEC 27001 Information Security Management Systems and the US National Institute of Standards and Technology's (NIST) Cybersecurity Framework) has also resulted in a largely harmonized and often well documented set of practices underpinning the cybersecurity profession. This is also reflected in recent efforts to classify cybersecurity technical capabilities under the international Cyber Body of Knowledge (the CyBOK) and various skills-based classification frameworks such as the European based Skills Framework for the Information Age (SFIA) and the NIST National Initiative on Cybersecurity Education's Workforce Framework for Cybersecurity.

The absence of a sophisticated, responsive globally harmonized regulatory environment causes friction across the many dimensions: legal and legislative, risk and business, research and development, innovative and technological, strategy and workforce. This is especially true for law-abiding cyber operators, and increasingly business directors and owners, who must navigate a patchwork of often rigid and sometimes point-specific rules often geared for cumbersome compliance-based activity. Depending on sector and circumstance, it may occasionally also force them to tread a fine line between legitimate and illegitimate outcomes within their home territory, let alone abroad.

Solving this challenge requires a multifaceted approach, as a harmonized cybersecurity regulatory environment must be fit for purpose against an ever-widening set of factors such as:

- **Zero day, current, and legacy cyber threats and vulnerabilities** and how these are quantified against strategic and operational risk, as well as how such risks compound over time into systemic risk[4];
- **The multitude and success of malicious actors**—from nation-states to large and small organized criminal syndicates to individuals—and the tactics, techniques and procedures they can deploy. Each can spoof, obfuscate, mimic and brute-force their way through the cyber-physical landscape—at times deliberately or inadvertently weaponizing regulatory drafting and enforcement, of particular concern in infra-structure developments and trade negotiations as well as for the global competitiveness of smaller nations and small business;

[4] World Economic Forum. "Systemic Cybersecurity Risk and Role of the Global Community. Managing the Unmanageable. Briefing Paper", Nov. 2022., https://www3.weforum.org/docs/WEF_GFC_Cybersecurity_2022.pdf

- **The asymmetric nature of malicious cyber activity** where defenses that are breached once in a hundred times have failed while attacks that work only once and never again are deemed successful;
- **The highly integrated nature of cybersecurity** with all other aspects of conducting day to day activities at the individual, organizational and jurisdictional levels, both in the technical and non-technical dimensions. This can make it difficult to prioritize cyber considerations over other compliance requirements;
- **Organizational context** such as sector (including government and academia), size and workforce awareness, business maturity and resilience, digital and physical supply and value chain dependencies, strategic and operational risk appetite and tolerances etc., as well as how such context impacts response and recovery from a successful cyber attack;
- **Intra- and inter-jurisdictional differences** in extant definitions, law and regulation in areas such as privacy, data retention and exchange, hosting infrastructure sovereignty, criminal conduct, export controls and trade, and product listings of what is considered dual versus multi-use at the crux of legitimate and illegitimate activity;
- **Rapidly evolving technological developments** require constant evolution of defenses and can render once highly effective cyber defensive activity obsolete as well as amplify risk within legacy infrastructure, processes and technology application;
- **National security and intelligence overlays** to cyber threats and risks blur the line between national and economic security and public and private responsibility.

These factors point toward the end goal: outcome-focused regulation that is consistent across nations. The pace, scale and reach of malicious cyber activity requires no less.

COMMON PRINCIPLES FOR HARMONIZATION

The principles outlined below were crafted to help policymakers align regulatory frameworks worldwide, and to develop regulations that drive good cyber. They also lay out the negative impact of conflicting requirements.

INTEROPERABILITY AND TRANSPARENCY

Interoperability is a foundational principle for harmonizing global cybersecurity regulations. It reflects the horizontal, interconnected nature of cybersecurity and emphasizes the need for cohesive, standardized approaches that facilitate effective cross-border cooperation.

The goal of interoperability is a trusted environment where organizations and nations can share threat intelligence, incident data, operational best practices as well as strategy and legal and lessons learned effortlessly, regardless of the specific regulatory framework(s) to which they adhere. Much like the practice of open source environments, a globally inclusive environment of regulatory interoperability would support scaled and enhanced information sharing by increasing access to authentic and peer-validated data, experiences and processes with appropriate contextual guardrails aligned to responsible behavior and global norms. Success is the development and adoption of rules that can easily and universally be updated and standards that enable governments, industry and individuals to maximize the scale of their cyber defenses across geographies. Common technical standards will also reduce the burden on businesses and agencies operating across borders and ensuring that compliance efforts are streamlined and more effective globally.

MARKET COMPETITION

A competitive market fosters the development of cutting-edge cybersecurity solutions (technologies, products and services), encourages continuous improvement, and provides consumers and business users with a diverse range of options. Regulations should avoid undue barriers to the global flow of data and technology, in part by formally recognizing the critical role of law-abiding defenders and organizational decisionmakers. This means avoiding policies that mandate the storage of data within national borders unless such measures are demonstrably necessary for national security or privacy reasons—and where this is deemed necessary, that transparency is employed. Similarly, nations must refrain from implementing regulations that infringe upon citizens' digital rights or create undue restrictions on access to information and services, placing onus on the opposite end of value chains to validate and verify legitimate use and application.

Regulations that promote open markets should also safeguard the intellectual property of cybersecurity solutions. Striking a balance between open competition and the protection of intellectual property, which can include defender tactics, techniques and procedures, ensures that industry is incentivized to develop and share new technologies while maintaining a fair and competitive market.

MUTUAL RECOGNITION

Mutual recognition frameworks will help avoid redundancy and streamline compliance efforts. This means recognizing that conformity to one set of regulations can satisfy the requirements of another, which in turn promotes efficiency and reduces compliance burdens. Mutual recognition agreements, such as those contemplated in the U.S.-EU Cyber Dialogue and contended by the African Union's Convention on Cyber Security and Personal Data Protection, offer a path to coherence in regulatory approaches.

Drawing parallels from law enforcement's principle of "concurrency," the principle extends to the mutual recognition of legal standards in cybersecurity. Where possible, nations should acknowledge and respect each other's legal frameworks, fostering an environment where compliance with one set of regulations is recognized as meeting the standards of another. This mutual recognition enhances global cooperation while respecting the diversity of legal systems.

CASE STUDY 1

UNHARMONIZED OPERATIONS: COORDINATING SEIZURE OF CRIMINAL DOMAINS

The lack of harmonization across legal and regulatory frameworks has real-life consequences. The cybercriminal ecosystem is composed of threat actors, victims, and infrastructure spread throughout the globe and to its participants is now generating trillions of dollars and causing hundreds of billions of dollars in follow-on consequences. Without harmonization, law enforcement's efforts to dismantle these organizations are at a significant disadvantage and are often rendered ineffective.

For example, in November 2016, a multi-national law enforcement operation dismantled a criminal organization that maintained an intricate, global network of tiered servers that provided so-called "bulletproof hosting" services to cybercriminals in return for a monthly fee. Dubbed the "Avalanche" network, it provided the world's most prolific cybercriminals with a hidden, secure platform from which to operate criminal schemes using more than twenty malware variants.

To dismantle the Avalanche network, law enforcement had to remove several million (predictable via algorithm) domain names from criminal availability. This involved seizing hundreds of thousands of already registered domain names and also preventing the registration of millions of yet to be created (so called "unborn") domains associated with each malware variant. Domains seized were directed to benign "sinkholes" able to enumerate the IP addresses of more than three million infected devices globally and facilitate international remediation efforts. The monumental challenge was how to seize and block these domains at registries and registrars located in more than 60 countries with vastly different, sometimes non-existent, legal authorities for such an undertaking.

Many countries had no mutual legal assistance treaties with those lead investigative countries seeking the domain seizures. Some countries had no domestic laws in existence that would permit the lawful seizure or blocking of malicious domains (such as the UK). Other countries were uncooperative with the US and European law enforcement agencies leading the operation and requesting the seizures/blocking.

The lack of harmonization among legal frameworks resulted in a time-consuming, labor-intensive effort by which a patchwork of solutions had to be created for each country and executed with 100% accuracy in order to ensure the operation's success.

The variety of solutions included certain countries serving criminal court orders on domestic registries and registrars, while other countries resorted to civil court orders. To effect seizures in foreign jurisdictions, some countries accepted and acted upon court orders issued in foreign jurisdictions, while others required time-consuming mutual legal assistance treaty requests seeking the recipient country to obtain legal process within their own jurisdictions. Countries with no domestic laws permitting domain seizures resorted to requesting registries and registrars to voluntarily action the domains pursuant to terms of service violations.

Without legal and regulatory harmonization across the globe, law enforcement's ability to timely and effectively disrupt cybercriminal activities is significantly challenged.

In uncooperative countries, registries and registrars actioned domains as a result of requests by private industry counterparts assisting in law enforcement operation. The success of the operation was as dependent on available legal process as it was on an informal network of compliant private and non-profit sector parties who thankfully chose to assist.

In short, the operation exemplified the extraordinary challenges presented by a lack of harmonization, as well as the meaningful successes that can be accomplished through effective public / private partnerships. Without legal and regulatory harmonization across the globe, law enforcement's ability to timely and effectively disrupt cybercriminal activities is significantly challenged.

WHY HARMONIZE?

The expanding threat environment over the past decade has made regulatory harmonization even more important. The gap between cyber risk and reward persists, with operational practices largely harmonized under technical standards like ISO/IEC 27001 and NIST's Cybersecurity Framework, while regulatory frameworks lag behind.

This discrepancy has led to rising friction across legal, legislative, risk management, business, research and development, innovation, and technological dimensions of society. It affects law-abiding cyber operators navigating a complex patchwork of often rigid and sector-specific rules. Inconsistent regulations and varying compliance standards allow malicious actors to seek out the gaps in the system and facilitate cross-border attacks.

Achieving a harmonized cybersecurity regulatory environment requires consideration of various factors. These include the dynamic nature of cyber threats and vulnerabilities, the diverse range of malicious actors, the asymmetric nature of cyber activities, the integration of cybersecurity into all aspects of daily activities, organizational contexts, intra and inter-jurisdictional differences, rapidly evolving technological developments, and the national security implications associated with cyber threats.

The first step is a minimum viable interoperability and mutual recognition of regulations between like-minded nations. The scale, pace, and reach of malicious cyber activities demand a more nimble and responsive approach to regulatory harmonization, which could be built on this foundation. The urgency at which this is needed now also goes beyond the scale and reach of today's and tomorrow's ever escalating cyber threat environment; the international community requires this first step in placewell ahead of the societal step change that will occur at the intersection of artificial intelligence and the commercialized quantum computer.

The benefits of such harmonization are significant:

RESILIENCE

Building cybersecurity resilience is a complex endeavor that cannot be accomplished in isolation or by governments alone. It demands a robust and inclusive governance model that actively involves not only public entities but also the private sector. This collaborative approach is essential to develop strategies and practices that safeguard our digital landscape and empower citizens to navigate the digital world securely. Building cyber resilience is a collective responsibility, and it necessitates a governance framework that unifies our response to cyber threats, empowers companies, and ensures the safety of our digital future.

SECURITY

Compliance is a necessary part of achieving the regulatory and voluntary objectives of security endeavors. Whether it is a government regulation or customer demand, requiring companies to show their homework is critical, including to support the trust that underpins interoperability. There are many cautionary examples of organizations marketing cybersecurity as a priority, only for a preventable compromise to expose a serious lack of diligence and embedded security culture. With mutual recognition, enterprises can begin to simplify the work done to secure systems and information. The breadth of unharmonized security requirements across jurisdictions creates a compliance exercise first, and a security imperative second.

EFFICIENCY, COST CONTAINMENT, AND CONSUMER BENEFIT

Harmonizing cybersecurity regulations will lead to fewer security and compliance requirements globally, allowing multinational companies to contain costs and gain efficiencies as well as for sectors and communities to more easily adopt the most effective cyber defenses. The reduced set of requirements will require less time and resources to chase down the differences between security and compliance baselines in different operating jurisdictions. This, in turn, opens the door for further competition due to interoperability and decreased barriers to market entry. These benefits and the associated lower costs can then be passed on to consumers.

CASE STUDY 2

THE FAIR ACT: A HARMONIZED MODEL FOR ASSESSING CYBER RISK IN THE FINANCIAL SECTOR

Financial services corporations globally have begun using cyber risk quantification (CRQ) through Factor Analysis of Information Risk (FAIR), currently the only international standard quantitative model for information security and operational risk.[5] With FAIR, an organization can establish risk-based cybersecurity and operational management policies, and adopt a standard taxonomy of security definitions, data collection criteria, measurement scales for risk scenarios, and criteria for developing an enterprise risk calculus. FAIR analysis is designed for compatibility with and to complement the existing risk management frameworks from organizations such as National Institute for Standards and Technology (NIST) and International Standards Organization (ISO).[6]

The new US Securities and Exchange Commission (SEC) rules on disclosure of material cyber incidents illustrate the potential practical utility of cyber risk quantification with respect to regulatory compliance activities. Many public companies, including multinationals providing services within various jurisdictions, are weighing options for how to determine if a cyber incident is material, and therefore reportable under the SEC rule. Using CRQ to estimate the financial loss associated with a cyber incident is a potentially promising contribution to these corporate decisions. Furthermore, CRQ can drive defensible prioritization of cyber risk mitigations based on high-risk outcomes, which would also help ensure compliance with regulations.

[5] The FAIR Institute. "What is FAIR?", 2024. https://www.fairinstitute.org/what-is-fair

"The FAIR Institute is a research-driven not-for-profit organization dedicated to advancing the discipline of cyber and operational risk management through education, standards and collaboration." The FAIR Institute has more than 500 member organizations.

[6] This informal input is agnostic on whether FAIR or another approach is preferable but recommends investigating CRQ as a means to account for advances in the rigor of risk measurement.

HOW TO HARMONIZE

The disjunction between the escalating cyber threat landscape and the evolution of regulatory frameworks has created an intricate web of challenges. While technical standards like ISO/IEC 27001 and COBIT 5 have achieved a level of operational harmony, the regulatory sphere lags, leading to a complex, sector-specific and geographically fragmented maze that poses challenges for multinational businesses and hampers coherent efforts to increase cybersecurity.

Recommendations for regulatory harmonization in cyber diplomacy involve intensified international cooperation, creating platforms for dialogue and collaboration. Despite the challenges posed by the lack of a universal international forum for meaningful convergence, increased bilateral and multilateral collaboration between nations is promising. Notably, the renewed EU-US Cyber Dialogues exemplify successful cooperation, providing a model for harmonization efforts beyond these regions.

Despite the challenges posed by the lack of a universal international forum for meaningful convergence, increased bilateral and multilateral collaboration between nations is promising.

The Joint CyberSafe Products Action Plan and discussions on mutual recognition of government-backed cybersecurity labeling programs exemplify EU-US leadership in this domain. Initiatives like the EU Cyber Resilience Act and the US Cyber Trust Mark showcase a commitment to common standards and will have a significant corollary impact on industry and government procurement practices as well as consumer behaviors. The formalized Working Arrangement between ENISA and CISA, covering cyber awareness and training, highlights strategic collaborative efforts with real and far-reaching positive change.

The G7 and regular observing nations should continue its effort to advance international security and stability in cyberspace, and cross-regional cooperation should be extended to Latin America, the Indo-Pacific, and Africa.

The G7 holds significant potential in fostering the harmonization of cyber requirements on the global stage:

- Member countries can enhance information sharing and collaborative efforts on cybersecurity.
- Member countries can support capacity-building initiatives, particularly in developing nations.
- Member countries can endorse and promote widely accepted frameworks, such as those developed by organizations like NIST and ISO, to encourage a harmonized approach to cybersecurity requirements.
- The G7 can also leverage its diplomatic channels to foster coordination and collaboration among member states and other nations. Regular dialogues, similar to the EU-US Cyber Dialogues, can provide a platform for discussing regulatory approaches, sharing experiences, and aligning strategies toward a more harmonized cybersecurity landscape.
- The G7 can promote collaboration between governments and private sector entities, encouraging the development and adoption of common cybersecurity standards across industries.
- The G7 can work toward aligning legal frameworks related to cybersecurity. This involves addressing legal challenges associated with cross-border data flows, cybercrime prosecution, and international cooperation in cyber crisis response.

The G7 Hiroshima Summit in 2023 focused on artificial intelligence (AI), and is a promising blueprint for how like-minded nations can seek to achieve regulatory harmonization in cybersecurity. Participants included Japan, Italy, Canada, France, the US, the United Kingdom, Germany, and the EU. Additionally, several additional nations were invited to the summit, reflecting a concerted effort to engage more broadly. Australia, Brazil, Comoros

(African Union Chair), Cook Islands (Pacific Islands Forum Chair), India (G20 Presidency), Indonesia (ASEAN Chair), Republic of Korea and Vietnam participated as invited countries. The summit also welcomed the presence of international organizations such as the UN, the International Energy Agency (IEA), the International Monetary Fund (IMF), the OECD, the World Bank, the World Health Organization (WHO) and World Trade Organization (WTO).

This diverse assembly showcased a collaborative initiative among nations and international organizations to address shared concerns. It led to an agreement by G7 leaders on International Guiding Principles on AI and a voluntary Code of Conduct for AI developers under the Hiroshima AI process. This collaborative spirit can extend beyond AI governance to cybersecurity, aligning regulations and policies among nations. The G7's commitment to supporting international organizations and multi-stakeholder initiatives, as highlighted in the summit, can translate into collaborative efforts seeking closer regulatory alignment in cybersecurity.

Standardization efforts should be bolstered, emphasizing the adoption of widely accepted technical standards. Collaborative initiatives, like those between Singapore, Finland, and Germany on the Cybersecurity Labelling Scheme (CLS), are encouraging.[7]

Achieving regulatory harmonization in cybersecurity demands a concerted effort at the global, regional, and national levels. The interconnected nature of the cyber landscape necessitates collaborative approaches that prioritize interoperability, market competition and mutual recognition. These principles can safeguard both national interests and global digital ecosystems.

[7] Singapore's Cyber Security Agency (CSA) has introduced the Cybersecurity Labelling Scheme (CLS) for consumer smart devices, the first of its kind in the Asia-Pacific region. The initiative rates smart devices based on their cybersecurity provisions, allowing consumers to make informed choices. Initially covering Wi-Fi routers and smart home hubs, it has expanded to include various consumer IoT devices such as IP cameras and smart door locks. The CLS encourages manufacturers to prioritize cybersecurity in product design. Singapore has signed agreements with Finland and Germany for mutual recognition of their cybersecurity labels, streamlining the certification process for consumer IoT products meeting the requirements of both countries.

EXEMPLAR:

COMPARING INCIDENT REPORTING IN HARMONIZED AND UNHARMONIZED WORLDS

The following table provides a snapshot of the realities of unharmonized vs. harmonized requirements for cybersecurity incident reporting.

REPORTING ELEMENT	**UNHARMONIZED REALITY** *Surveying the multitudes of security baselines across the globe.*	**HARMONIZED BEST PRACTICE** *NIS2 in the European Union (Applicable to 27 member states and mid- and large-sized companies providing services or carrying out activities in any country in the European Union)*[8]
DEFINITION OF A REPORTABLE CYBER INCIDENT	Existing regulatory frameworks have employed different language to define reportable cyber incidents or otherwise describe the threshold of what is reportable. One key divergence in existing regimes is how they characterize the impact of incidents that must be reported. Examples include: **"substantial loss," "disruption," "severe operational disruption," "material or non-material damage," "potential adverse effect," and "serious impact."** Each of these thresholds envisions some impact before reporting is required, but they all can be interpreted to define "reportable" cyber incidents.	NIS2 requires reporting when an incident is considered "significant" in that it "**has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned**" (Article 23(3)(a)) or "**if it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage** (Article 23(3)(b))."

[8] "Consolidated text: Directive (EU) 2022/2555 of the European ParliamentLex - 02022L2555-20221227 - En - EUR-Lex." *EUR-Lex Access to European Union law*, eur-lex.europa.eu/eli/dir/2022/2555.

REPORTING ELEMENT	UNHARMONIZED REALITY	HARMONIZED BEST PRACTICE
REPORTING TRIGGERS AND TIMELINE REQUIREMENTS	Divergent timelines and triggers for reporting cyber incidents also result in unharmonized cyber incident reporting. Reporting timelines for national or economic security regimes may include: **"immediately," "promptly," "one hour," "24 hours," to "72 hours" or "without delay."** In contrast, reporting for privacy and consumer protection incidents may have longer timelines such as a specified number of business days with a cut-off. There are also "tiered" reporting timelines, where entities report either sooner or later based upon the severity of the impact or significance of the impacted system. Tiered reporting timelines can also be based upon the amount of data exposed in the context of privacy and consumer protection focused regimes.	NIS2 provides that organizations should send an "early warning" **within 24 hours of becoming aware of a significant incident**, followed by an "incident notification" within 72 hours and a final report one month after the incident notification. It outlines subsequent reporting requirements as time goes on and more information is discovered.
REQUIRED REPORTING PLATFORMS & INFORMATION SHARING	Across incident reporting regimes, there are wide disparities in terms of reporting mechanisms adopted. These online submission systems consist of: **"web forms," "web portals," "secure file transmission systems," or "forms submitted via email."** Other incident reporting regimes accept reports through more traditional mechanisms like: **"email messages," "mail," "fax," or "phone communications."** The diversity in reporting mechanisms increases the challenges associated with normalizing and analyzing data that is reported and harmonizing the reporting process across incident reporting regimes.	NIS2 requires notification to the **computer security incident response team (CSIRT)** or a competent authority (as designated by each Member State and their agency or organization responsible for cybersecurity) These entities and reporting contact information have been compiled at https://csirtsnetwork.eu/ for transparency and ease of use.

REPORTING ELEMENT	UNHARMONIZED REALITY	HARMONIZED BEST PRACTICE
FINAL REPORT REQUIREMENTS FOR AN INCIDENT	Various incident reporting regimes include different requirements in terms of the types of information that must be submitted as part of an incident report. For example, some incident reporting regimes require a final report to complete the record or communicate that an entity considers the incident resolved. Others only require an initial notification of an incident or an initial incident report with the possibility of follow-on touchpoints to supplement or amend what has already been submitted.	For a significant incident, NIS2 requires: 1. An early warning (24 hours after knowledge of incident) 2. An incident notification (72 hours after knowledge of incident) 3. A final report (not later than one month after the incident notification) The European Commission is tasked with specifying in implementing legislation the type of information, format and procedure to be followed for notifications.
LIABILITY PROTECTIONS AND DATA PROTECTION	Inconsistency in current information protection regimes is resulting in unharmonized liability and data protections. There is a lack of consistent standards and guidance for how reported cyber incident information is protected or shared between national or international authorities. Reporting entities may find that the same information is subject to different information protections or use limitations when submitted to multiple agencies and that the protections they receive may be dependent on the agency to whom they submit the report.	Under NIS2, member states "shall ensure that the **exchange of information takes place within communities of essential and important entities**. Such exchange shall be implemented through **cybersecurity information-sharing arrangements** in respect of the potentially sensitive nature of the information shared." NIS2 also provides that "[t]he mere act of notification shall not subject the notifying entity to increased liability."

CONCLUSION

It is not a question whether governments are going to regulate cybersecurity; they are and they will. The question is whether the regulations they develop will be effective, and increasingly, whether the regimes that support them can be flexible enough to keep pace with continued step changes in technology and their myriad resulting applications.

But crafting effective regulation is not easy, and developing regulations that are harmonized across national boundaries is even more complicated. It is possible, though, and the principles set out above can help guide policymakers on that path. Further, these principles can guide industry and academia's engagement with policymakers to assure trusted, considered yet appropriately paced iterations and evolutions in policy and practices.

Pursuing common, consistent approaches is essential to harmonizing regulations; to the extent a country can promulgate rules that are consistent with other nations, the more likely it is that industry and others can (and will) comply. Conversely, when a regulation differs greatly from the norm, it is hard for an impacted party to adjust its conduct accordingly—whether the party is an individual, an informal collective, an organization (of any size or sector), or intra-nation. And if the rules contradict those of another country, it can put an organization in the impossible situation of having to pick which laws to violate and which to follow, the examples of which are endless even before considering what organizations are compelled to do in situations of cross-border civil or military unrest.

Effective regulation will harness market forces to achieve the desired policy outcome; where the market has "failed" to drive better practices, government policy can shift those market pressures. This works best when regulation drives innovation toward a policy goal and does not create artificial geographic barriers or missteps in legal interpretation and application of best practice operating models.

It is important to note that the biggest market of all is that operated by malicious cyber actors—when collective efforts to shift market pressures are successful in the legitimate arena, this can also have a sustained and measurable impact on the illegitimate area if we are harmonized.

Finally, before developing new or novel regulations, policymakers should see if other jurisdictions (whether in their countries or internationally) have already done so and where possible borrow from that work. Imitation is more than the highest form of flattery—it is the best path to effectiveness.

Unfortunately, the benefits from harmonized regulation are still largely unfelt, because to date cybersecurity regulation has been siloed. But the downside of inconsistent, conflicting regulation is very real. As described above, law enforcement struggles to cooperate across border to stop cyber criminals and companies spend resources complying with myriad conflicting breach regulations rather than protecting against breaches or innovating. This paper provides a starting point on fixing that, for industry and governments alike, and free up much needed capacity to lean toward the next big challenges cybersecurity regulation faces in the future.

ACKNOWLEDGMENTS

This paper was developed through virtual meetings of the Regulatory Harmonization working group from May 2023 to January 2024.

OBJECTIVES

This paper sets out to establish regulatory harmonization principles that are broadly applicable to help frame conversations between governments and industry that can lead to streamlined and consistent standards, regulation, and legislation.

CONTRIBUTORS

Cecilia Bonefeld-Dahl
Co-chair

Michelle Price
Co-chair

Matt Bodman
Cameron Byrd
Tod Eberle
Katherine Fang
Stew Garrick
Iranga Kahangama
Rob Strayer

ASPEN DIGITAL TEAM

Jeff Greene
John Carlin
Katie Brooks
Devon Regal

ASPEN GLOBAL CYBER GROUP MEMBERS May 2024

David Koh
Co-chair

Corey Thomas
Co-chair

Yasmin Brooks
Co-chair

Jorge Guajardo
Co-chair

Dmitri Alperovitch
Paul Ash
George Barnes
Carl Bildt
Christophe Blassiau
Cecilia Bonefeld-Dahl
Yasmin Brooks
Inge Bryan
Paolo Dal Cin
Oleh Derevianko
Anriette Esterhuysen
Tobias Feakin
Camille Francois

Stew Garrick
Katherine Getao
Dario Gil
Ron Green
Jane Horvath
Mikko Hypponen
Chris Inglis
Marina Kaljurand
Boon Hui Khoo
Tzipi Livni
Ciaran Martin
Chris Painter
Guillaume Poupard

Michelle Price
Greg Rattray
Latha Reddy
Runa Sandvik
Rob Strayer
Eli Sugarman
Yigal Unna
Phil Venables
Grant Verstandig
Alicia Wanless
Alberto Yepez
Shinichi Yokohama

Individuals are encouraged to cite this report and its contents. In doing so, please include the following attribution:

"A Security Symphony." Aspen Digital, a program of the Aspen Institute, May 2024. CC BY-NC. https://www.aspendigital.org/report/security-symphony

Global Cybersecurity Group | ASPEN DIGITAL

aspen institute