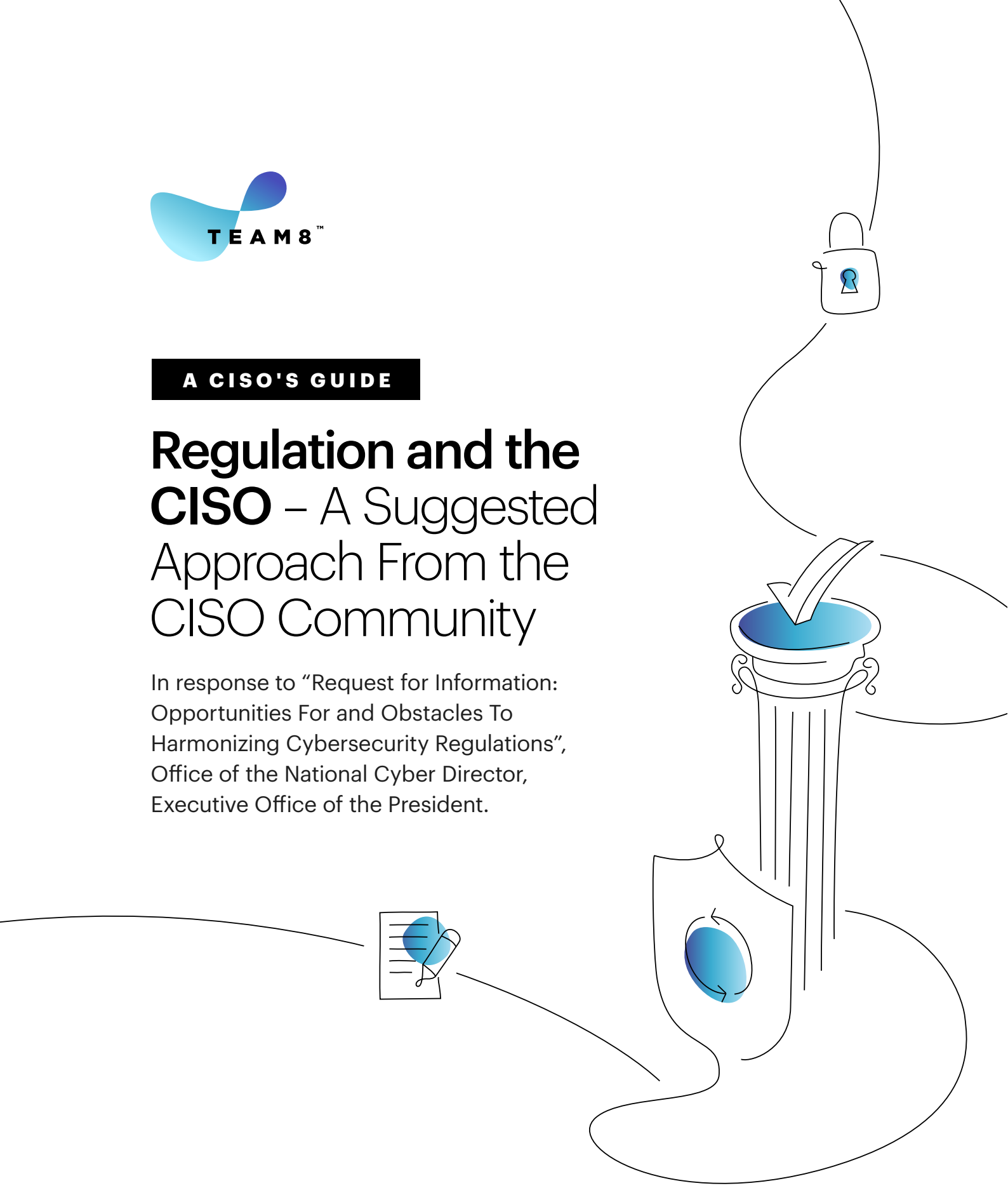
TEAM8™

A CISO'S GUIDE

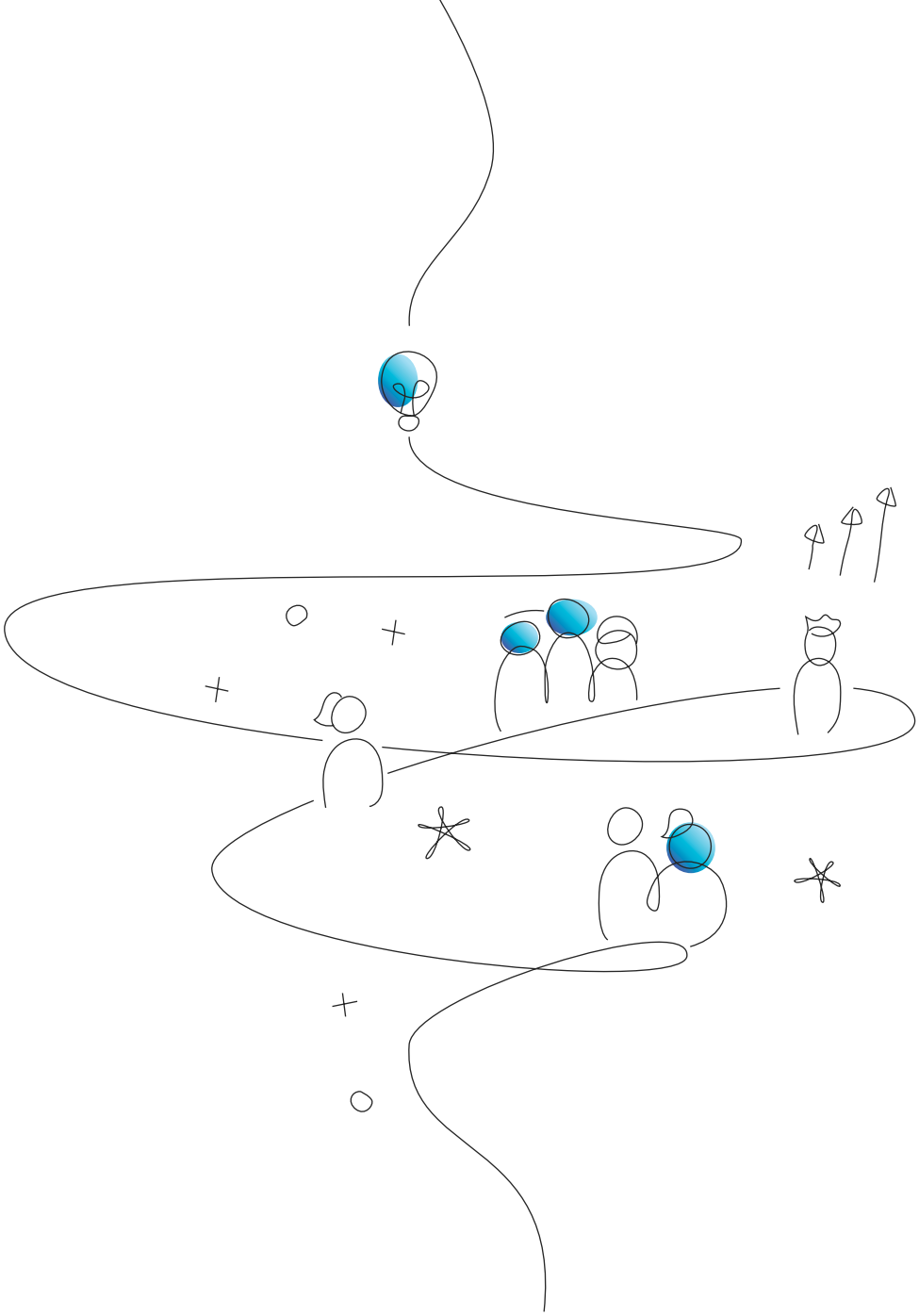
Regulation and the CISO – A Suggested Approach From the CISO Community

In response to “Request for Information: Opportunities For and Obstacles To Harmonizing Cybersecurity Regulations”, Office of the National Cyber Director, Executive Office of the President.



By the Team8 CISO Village

September 2023



The Team8 CISO Village is a community of CISOs from the world's leading enterprises. The primary focus of the Village is to facilitate collaboration among the world's most prominent companies with the goal of sharing information and ideas, conducting intimate discussions on industry and technology trends and needs, and generating value and business opportunities for all parties.
By helping Team8 to identify real pain points and understand the requirements of large organizations, members of the Village are first in line to leverage solutions that are purpose-built by Team8's portfolio companies to support their needs.

To contact the Team8 CISO Village, please email **cisovillage@team8.vc**

WRITTEN BY

Chris Inglis

Former US National Cyber Director (2021-2023)

Gadi Evron

CISO-in-Residence
Team8

Amit Ashkenazi

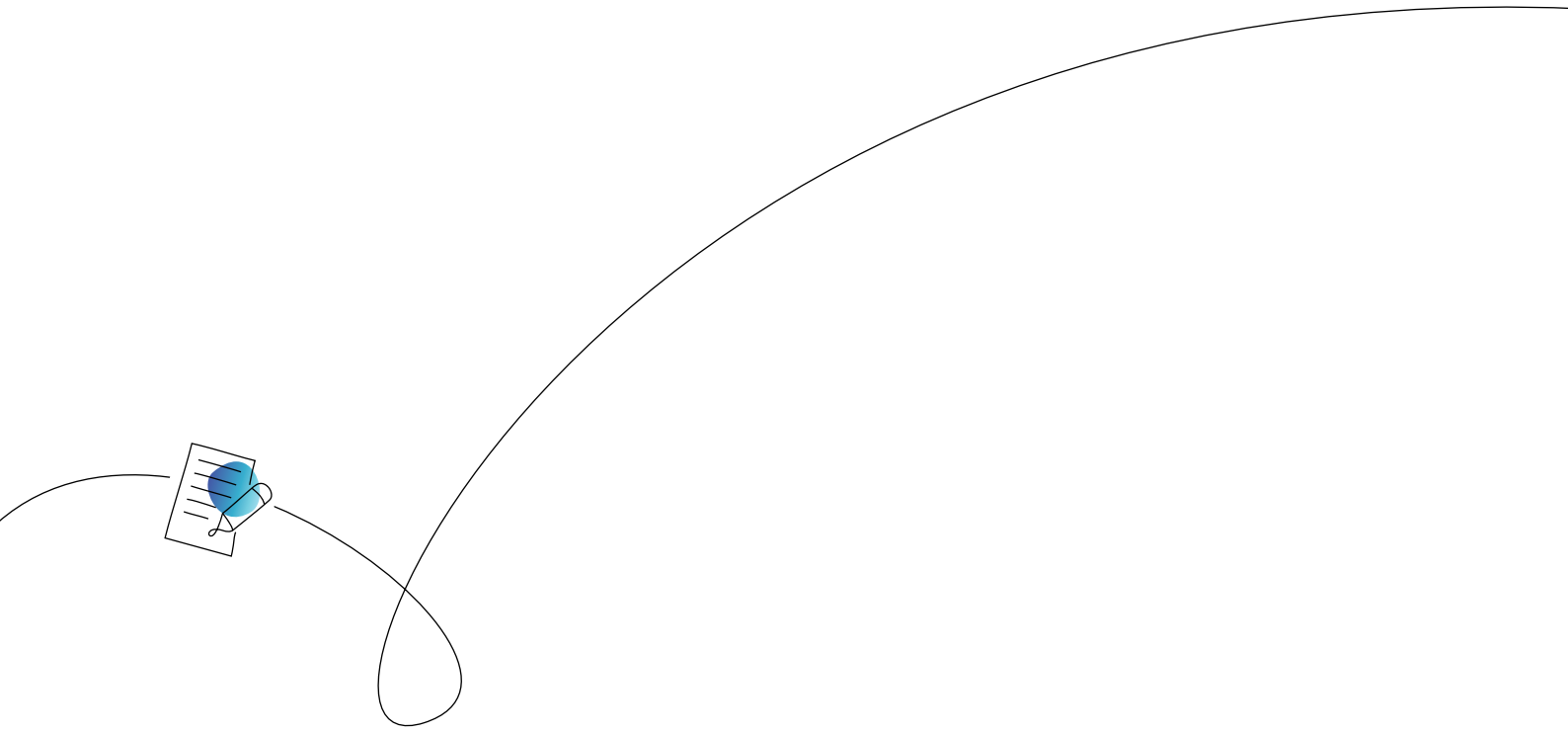
Former Legal Advisor of the Israel National Cyber Directorate, and before that Head of the Legal Department at Israel's Privacy Protection Authority

CONTRIBUTORS AND SIGNEES

Many Team8 CISO Village members, and others from the wider community, assisted in the writing, reviewing, and editing of this document. These are the ones who could share their names publicly: **Amir Zilberstein, Ángel Uruñuela, Ariel Litvin, Bill Nelson, Billy Spears, Bobi Gilburd, Charles Blauner, Christoph Peylo, Chuks Ojeme, David Fairman, Gal Tal-Hochberg, Gary Johnson, Gary Hayslip, Herman Young, Ian Lilleby, Israel Bryski, Jason Woloz, Josh Lemos, Kim Perrin, Liran Grinberg, Mark Orsi, Michael S. Rogers (ADM USN, ret), Nadav Zafrir, Pat Choy, Phil Beyer, Rich Lindberg, Rohit Parchuri, Shaun Marion, Shawn Bowen, Shinichi Yokohama, Susanne Senoff, Thomas Heuckeroth, Tim O'Brien, Timo Wiander, Travis Farral, Valmiki Mukherjee, Yoni Efrati.**

INTRODUCTION

The Team8 CISO village[1] commends the White House Office of the National Cyber Director (ONCD) on its approach to cybersecurity regulation, and its timely "Request for Information on Cybersecurity Regulatory Harmonization".[2] In this submission, we would like to stress the importance of a comprehensive new approach to regulation, based on "agile regulation" and focusing on the role of the CISO community, its concerns, and its contributions to better cybersecurity.



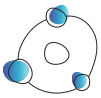
[1] Team8 Group is a global Company-Building and Venture Capital group that creates and invests in companies focusing on Cybersecurity, Data & AI, Fintech, and Digital Health. The Team8 CISO Village is a community of +350 CISOs from the world's leading enterprises. The primary focus of the Village is to facilitate collaboration among the world's most prominent companies with the goal of sharing information and ideas, conducting intimate discussions on industry and technology trends and needs, and generating value and business opportunities for all parties. The Team8 Village is an essential part of Team8's unique company-building model.

[2] White Office of the National Cyber Director, Request for Information on Cybersecurity Regulatory Harmonization, https://www.whitehouse.gov/wp-content/uploads/2023/07/ONCD-Reg-Harm-RFI-Final-July-19.2023.pdf. We believe that the "Request for Information" published by ONCD is timely and essential for any further regulatory effort.

Key Points

The National Cybersecurity Strategy has set ambitious goals for changes in cybersecurity regulation. we support the government's desire to improve the security of the industry, and safety of our customers and citizens. To achieve these goals, it could benefit from a new regulatory approach.

Regulation, when introduced, needs to be harmonized amongst regulators, and to achieve regulation that meets the standard of a "lightest possible touch but no lighter". Regulatory strategy should encompass all the stakeholders, including technology providers that are sometimes the critical weak link.



Developing a new regulatory ecosystem, based on concepts of "agile regulation" can produce game-changing solutions for current cybersecurity challenges.

A key element of this new regulatory ecosystem is engaging the Chief Information Security Officer (CISO) community in a continuous dialog based on trust, shared values, and knowledge proliferation.

Rules should be sensitive to the differences between the roles and responsibilities of corporate leaders, CISOs, and other frontline defenders in particular. These rules should also provide CISOs adequate protections from legal exposure when appropriate.

Expectations from the CISO under existing and new regulations need to be clear, realistic, and coherent across government regulatory activities without creating unnecessary burdens to an already challenging role.

The importance of effective CISO engagement is even more crucial to reduce cybersecurity legal exposure in the age of AI. To enable organizations to harness the benefits from this developing new technology, CISOs and regulators need to cooperate to ensure adequate, effective and non excessive risk management and mitigations.

CONTENTS

01

Effective Cybersecurity regulation: **"Lightest possible touch and no lighter"**

Cybersecurity is a complex discipline that requires tailoring technical knowledge and threat assessments to organizational operational needs. It depends on correctly prioritizing mitigation measures and its ability to affect organizational culture.

Regulation of cybersecurity is challenged by the quick pace of technological change, constantly evolving threat scenarios, and the difference in knowledge and expertise between regulated entities and their regulators. While regulation can affect incentives to invest in cybersecurity, it can lead to a "checkbox" compliance attitude, that focuses effort on minimizing legal exposure rather than actual cybersecurity exposure. Regulation can also have a chilling effect on cyber defenders, that already many times find CISOs selves needing to juggle immediate threat-based decisions while dealing with other organizational stakeholders and legal exposure.

In this paper we offer suggestions to deal with these challenges and develop more effective regulation. We would like to elaborate on how achieving the National Cybersecurity Strategy's goals of **"fundamental shifts"** in allocation of **"roles, responsibilities, and resources in cyberspace"**,[3] could benefit from a change of regulatory mindset.

As a preliminary note, we suggest that to minimize these challenges in the first place, regulation should meet the standard of "lightest possible touch but not lighter". In addition, regulation should be harmonized amongst regulators, so as to reduce compliance costs, focusing our cyber security dollars on controls, measures, and testing, as well as avoiding the challenge presented by the slightly different regulatory documents being developed by multiple states and countries.

Regulatory strategy should make sure responsibility is allocated effectively to all the stakeholders, including technology providers that are, on more than one occasion, the critical weak link.

[3] See White House, Fact Sheet: Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan, July 13, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/: "President Biden has made clear that all Americans deserve the full benefits and potential of our digital future. The Biden-Harris Administration's recently released National Cybersecurity Strategy calls for two fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace:
1. Ensuring that the biggest, most capable, and best-positioned entities – in the public and private sectors – assume a greater share of the burden for mitigating cyber risk
2. Increasing incentives to favor long-term investments into cybersecurity"

02

New regulatory approach: **"Agile regulation" and the importance of trusted dialog**

Key points

1. Agile regulation[4] is a comprehensive new approach to regulation, aimed at developing regulation that better adapts to the quick pace of market or technological changes.
2. Agile regulation is based on "adaptive, iterative, and flexible regulatory assessment cycles"[5] and evidence based advanced regulatory management tools which include regulatory impact assessment and ex post evaluations.[6]
3. In the context of agile regulation, a trusted dialog with the CISO community can achieve the following benefits:
    a. Regulators can see different and real world implications of technical and legal rules.
    b. CISOs can benefit from getting relevant support from government.
    c. Regulatory goals and measures are clearer and better communicated which can improve compliance.
    d. Contradictory regulatory requirements can be located and deconflicted.
    e. Cross sector and international friction between different cybersecurity measures aimed to achieve the same goals can be streamlined.

Developing regulation for cybersecurity requires dealing with the quick changes of technology and the risk environment, as well as creating rules to affect organizational behavior. To deal with these challenges, regulatory strategy should go beyond allocating liability and develop fresh cybersecurity regulatory approaches based on concepts of "agile regulation".

Agile regulation[7] is based on "adaptive, iterative, and flexible regulatory assessment cycles"[8] and evidence based advanced regulatory management tools which include regulatory impact assessment and ex post evaluations.[9] It aims to deal realistically with the challenges of developing regulation and deploying it in a timely manner. Within this new concept of regulation, a trusted public private professional dialog is a key element. In this dialog, the CISO community, as the subject matter experts and professional pillars of cybersecurity in organizations, plays an essential role. A trusted dialog with the CISO community can help solve some of the challenges of cybersecurity regulation. It helps mapping gaps in technical knowledge and

[4] Based on evolving concepts of "agile regulation" See: Organization for Economic Cooperation and Development, Recommendation of the Council for Agile Regulatory Governance to Harness Innovation, 06.10.2021, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464, ("OECD Recommendation").

[5] See OECD Recommendation section II (1).

[6] See OECD Recommendation, section I.

expertise, as well as organizational approaches to risk management, Information and Communication Technologies (ICT) management, and cybersecurity management. It supports flagging inconsistencies between cybersecurity regulatory requirements in the US,[10] and between US requirements and international regulation.

We suggest that developing a modality for continuous government engagement with the CISO community at large, including harnessing digital technology for this goal,[11] should be a key priority. CISOs are employed at many types of organizations, and the insights of Fortune 500 as well as Small and Medium-sized Businesses (SMBs) CISOs are different but no less important. Engagement should aim to be inclusive of the diverse views and angles of the cybersecurity craft. We are of course aware of the important work done at the CISA CISO advisory board – but we believe this type of engagement is not enough and can benefit from engaging larger communities. An open dialog throughout the development and deployment of regulation could help clarify regulatory goals and measures, ensure they are a good fit for intended purpose, and ultimately improve compliance.

While it is an accepted practice by regulators to publish draft regulations and even have "town hall" meetings, there are still loopholes in the process. In some cases, it is unclear what the government does with comments sent to it. In other cases, final rules are still not completely clear and do not have a simple explanatory support mechanism. More ways to engage with the CISO community at large could bridge these gaps.

[7] See: Organization for Economic Cooperation and Development, Recommendation of the Council for Agile Regulatory Governance to Harness Innovation, 06.10.2021, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464, ("OECD Recommendation").

Agile regulation aims to develop new regulatory modalities that balance between the need to protect important public interests in areas of high risk and uncertainty, while recognizing the importance of innovation.

This type of approach is similar to the way regulatory policy for Artificial Intelligence is developing under the coordination of the White House. See: White House, Executive Office of the President, Office of Management and Budget, M-21-06, Memorandum for the Heads of Executive Departments and Agencies – Guidance for Regulation of Artificial Intelligence Applications, November 17, 2020, https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/11/M-21-06.pdf

[8] See OECD Recommendation section II (1).

[9] See OECD Recommendation, section I.

[10] In the area of data privacy, as an example, see: Anokhy Desai, US State Privacy Legislation Tracker, IAPP, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

[11] See: Admin. Conf. of the U.S., Recommendation 2023-2, Virtual Public Engagement in Agency Rulemaking, 88 Fed. Reg. 42,680 (July 3, 2023).

An open dialog could also inform the development of dedicated effective policy and regulatory measures, while reducing unintended consequences and burdens on innovation. It would allow understanding common challenges and opportunities for effective government support and intervention. One such example is the CISA "Cross-Sector Cybersecurity Performance Goals" which help operationalize and prioritize organizational risk management.[12]

In the wider regulatory context, the effect of such an approach can reduce inconsistencies between the myriad of existing and quickly developing regulatory requirements.

A dialog with the CISO community, which many times needs to operate in multiple jurisdictions, can support the government's efforts to streamline and consolidate regulation as well as enrich international deliberations. The challenges of the existing regulatory and risk environment are multiplied in the age of AI, and require CISOs and regulators to adapt.[13]

[12] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[13] See: Team8 CISO Village, A CISOs Guide: Generative AI and ChatGPT Enterprise Risks, April 18, 2023, https://team8.vc/rethink/cyber/a-cisos-guide-generative-ai-and-chatgpt-enterprise-risks/.

03

New regulatory ecosystem: The CISO and fostering cooperation

Key points

1. Effective cybersecurity regulation can benefit from a new regulatory ecosystem that helps the CISOs in carrying out their jobs.
2. A new regulatory ecosystem means:
   a. Reducing regulatory burden and risk to CISOs
   b. Recognizing different points of view while encouraging dialog.
   c. Encouraging cooperative projects to develop cybersecurity knowledge and tools, such as joint professional skills development.
   d. Following up on regulation with "practice guidelines", implementation feedback loops, and revisions and updates as necessary.

CISOs are the professional pillar of cybersecurity in organizations, and also have a challenging organizational role. They need to deal with state of the art technology, adversary risk, internal risk, and engage with all levels of the organization. They support organizational efforts to reduce legal and regulatory exposure. In some fields of organizational activity, regulatory requirements overlap, and require adaptation. Sometime, such as during an investigation of a potential breach, several government organizations may be involved. Each of these tasks and relationships can create tensions and stress for the CISO, who needs to navigate these difficult issues carefully. Recent events have raised the level of organizational and personal exposure for the CISO role.

New cybersecurity regulatory obligations, means more professional pressure and potential legal exposure for the CISOs in their different roles. These challenges can make the CISO less effective in their role, and shift overall efforts to dealing with legal exposure instead of cybersecurity exposure.

To deal with these challenges, regulators should consistently take into account these tensions. While the White House RFI to map regulatory requirements is a welcomed first step, we suggest a wider approach that reduces regulatory burden and supports the CISOs in their role.

Addressing CISO concerns and promoting cooperation: Reducing regulatory burden and risk to CISOs

The organization's key personnel for dealing with outside legal and compliance risk are the legal advisor and the compliance officer. However, because of the technical nature of cybersecurity risk, CISOs may find CISOsselves amid these legal discussions, including with regulators.

Regulators need to consider these organizational dynamics and the effect of regulatory rules and interactions on CISOs. It is advised that rules should enable CISOs to operate comfortably within their professional domain, including open channels of communication with government agencies.

Thus rules that can affect this domain, such as those that apply to information shared by a CISO during a cyber event, should be clarified, including with which government agencies the information will be shared, and what the agencies are allowed to do with this information. Limiting the use of the information enables companies to share more quickly, before all of the details have been verified.This is especially true in cases where regulatory requirements may create personal exposure to CISOs, in a way which may stifle some of their activities.[14]

Rules should be sensitive to the differences between the roles and responsibilities of corporate leaders, CISOs, and other frontline defenders. These rules should also provide CISOs adequate protections from legal exposure when appropriate. Especially, rules that apply to CISOs need to be clear, coherent across government activities, and not counter productive to the CISO role.

Recognizing different points of view while encouraging dialog

Regulators oversee protection important public interests, and would like to make sure that organizations invest proper efforts in cybersecurity. However, they can benefit from insights as to the real-world implications of regulatory measures on cybersecurity.

Regulators should be encouraged to develop and deploy regulations that are "fit for purpose" – one that solves problems rather than resorts to a "ticking the box" exercise.

Regulators should be aware that organizations are not all the same, and thus engagement needs to take into account the different sizes, digital sophistication, and maturity of risk governance of organizations in which CISOs operate.

More so, the government should distinguish between input received from technology vendors, especially some of the larger companies, and the rest of the ecosystem. Indeed, some of the challenges that CISOs need to deal with can be better addressed by a more accountable and trustworthy supply chain.

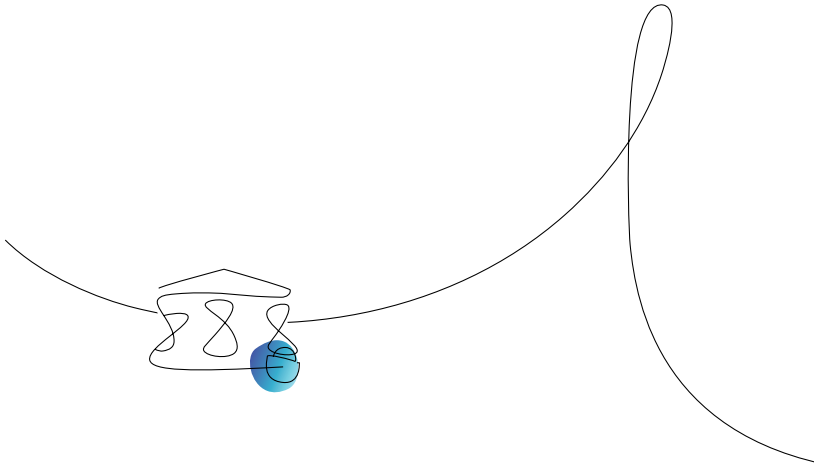
One way to achieve these goals is encouraging cooperative projects to develop cybersecurity knowledge and tools, such as joint professional skills development.

[14] We discuss this in more detail in our CIRCIA submission, Team8 CISO Village, CISO Community Recommendations in Response to CIRCIA, 30.03.2023, https://team8.vc/rethink/cyber/ciso-community-recommendations-in-response-to-circia/.

Creating a continuous dialog: "Practice guidelines", implementation feedback loops, revisions, and updates as necessary

Given the quick pace of change in technology and risk, regulators could benefit from feedback loops between CISOsselves and CISOs to iterate and evaluate the real world implications of technical rules. While many times regulators publish documents for comments, after publication some regulations remain unclear and create compliance risk. Other regulations may become out of date, but due to lack of regular review cycles, they remain in effect.

Developing a support mechanism for regulation, implementation feedback loops, and regulatory expiry dates could help align regulation with developing technologies, threat scenarios and mitigation best practices.



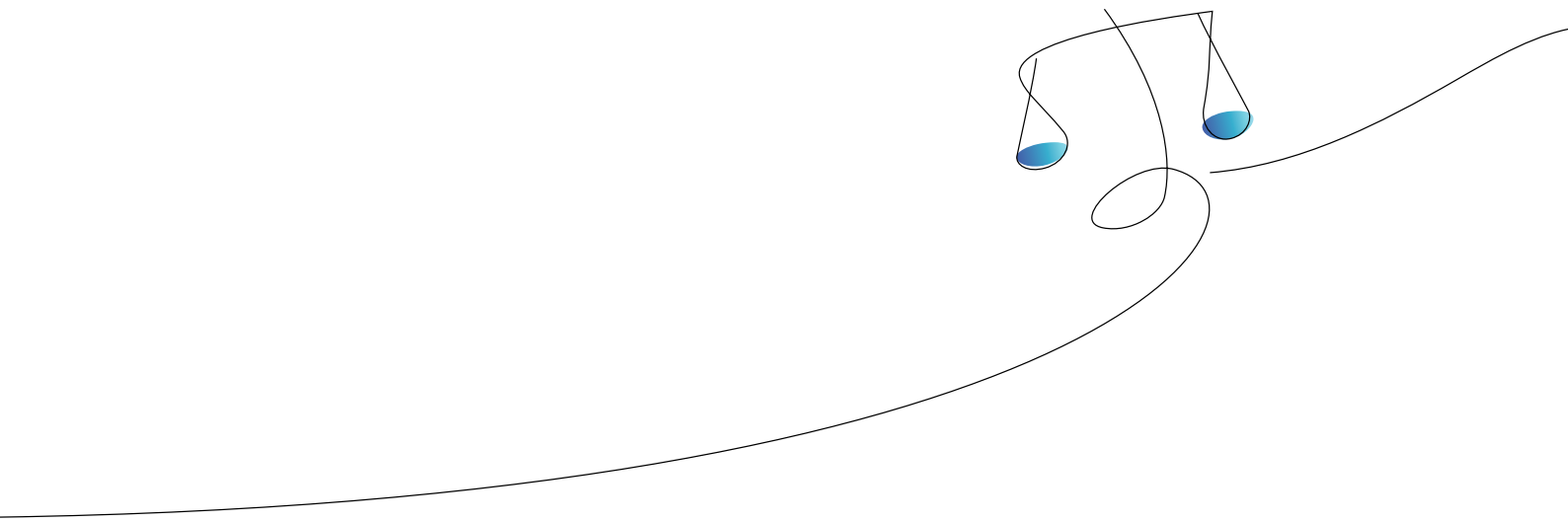
CONCLUSIONS

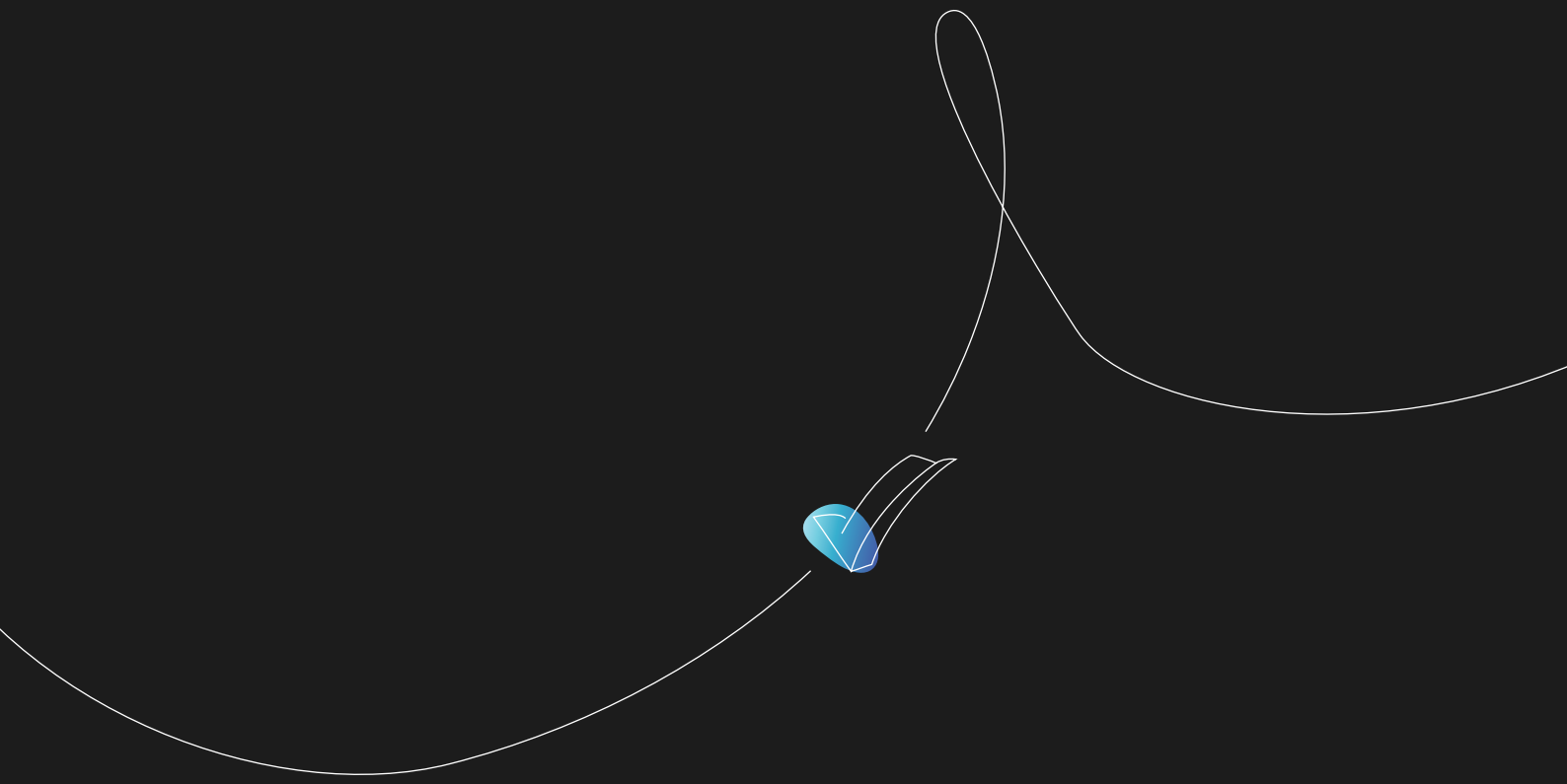
The National Cybersecurity strategy calls for "fundamental shifts" in allocation of "roles, responsibilities, and resources in cyberspace", while both aiming for a greater share of the burden of mitigating risk by the private sector and increasing incentives for long term investment in cybersecurity. We support the government's desire to improve the security of the industry and safety of our customers and citizens. We think that this strategy will help make these goals achievable.

The importance of effective CISO engagement is even more crucial to reduce cybersecurity legal exposure in the age of AI. To enable organizations to harness the benefits from this developing new technology, CISOs and regulators need to cooperate to ensure adequate, effective, and non excessive risk management and mitigation.

To achieve these ambitious goals requires a change of regulatory mindset, one that recognizes the complex nature of the cybersecurity mission, spanning technical knowledge, economic incentives, and affecting organizational culture.

This new regulatory mindset can benefit from concepts of "agile regulation" to create a new regulatory ecosystem. A key element of this new regulatory ecosystem can be creating frameworks that engage the CISO community without creating excessive legal or regulatory exposure.





For more information

Contact us at: cisovillage@team8.vc | www.team8.vc

TEAM8™