In collaboration with
Global Resilience Federation

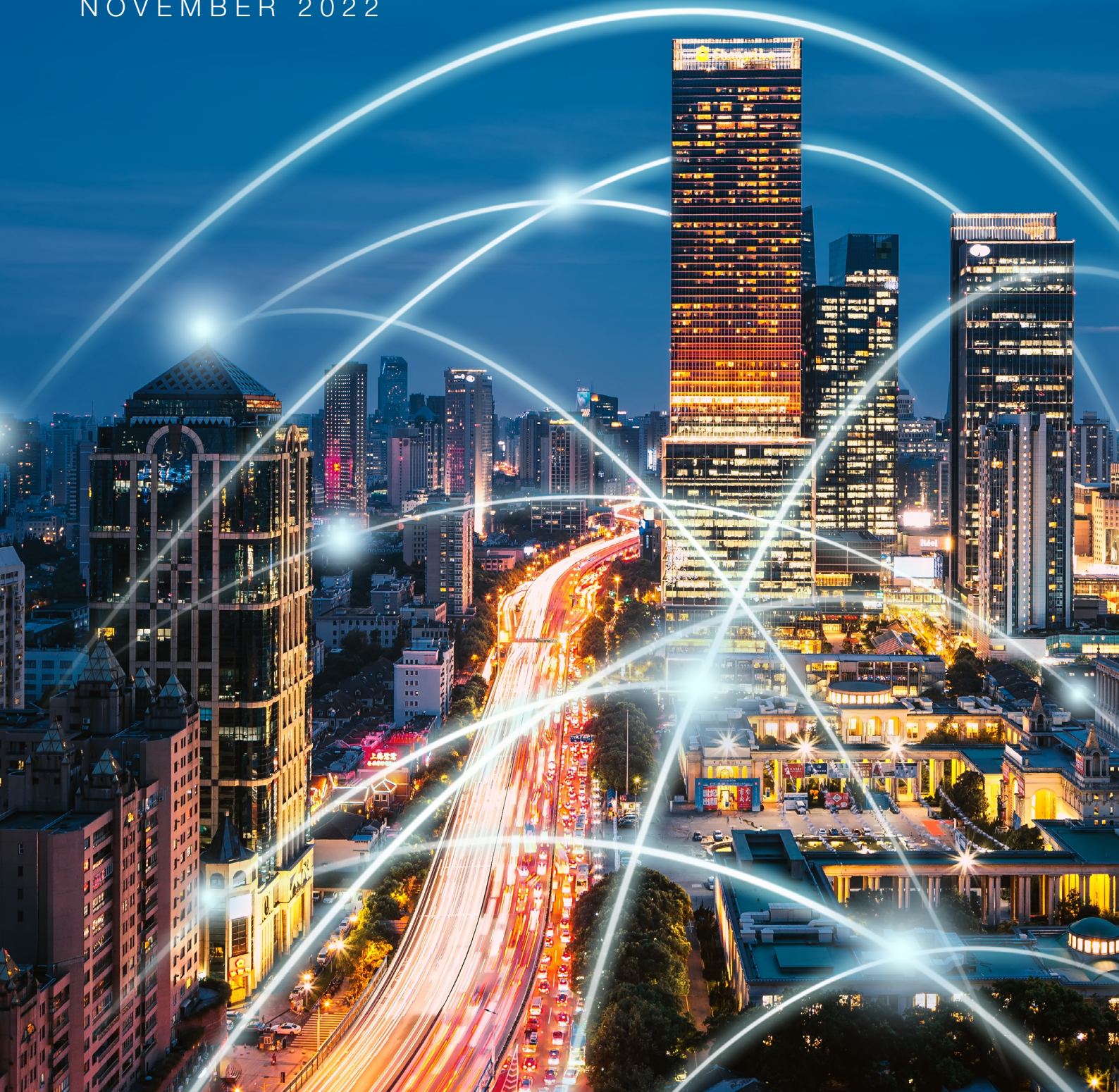
Partnership against Cybercrime

WORLD ECONOMIC FORUM

The Business Imperative of Cyber Information Sharing for Our Collective Defence

COMMUNITY PAPER

NOVEMBER 2022



Cover: Mars Yu, Getty Images – **Inside:** Getty Images

Contents

Foreword

Charles Blauner
Special Adviser, Global Resilience Federation

Michael Daniel
President and Chief Executive Officer, Cyber Threat Alliance

Jeremy Jurgens
Managing Director, World Economic Forum

Why are we still talking about cyberthreat information sharing? It is not a controversial topic. Cybersecurity professionals almost universally support increased information sharing. Scores of reports have endorsed the concept, and government policies promote the idea. Entire organizations exist to enable it. In fact, the consensus on information sharing is remarkable for its consistency and durability. Yet, despite this consensus, the level of cyberthreat information sharing remains insufficient. Cleary, if everyone agrees that we should do something, but many organizations do not, we need to examine the impediments to action more closely. Most importantly, we need to think about the topic differently.

This paper, "The Business Imperative of Cyber Information Sharing for Our Collective Defence", provides such an alternative perspective. Critically, it does not make the case for information sharing based on altruism or patriotism or on technical grounds – traditional arguments for increased sharing. Instead, it makes the case based on economics. In today's world, if a business wants to thrive (or even survive), then it must successfully manage its cyber risk. In turn, effective risk management requires cyberthreat information sharing. By tying information sharing to a business imperative, this paper uses a language that business leaders understand and regularly act upon.

Of course, legal issues, cultural barriers and an unclear return on investment can still hinder sharing even if business leaders recognize the imperative. This paper also addresses these problems. It lays out a practical, three-step method for overcoming the barriers to sharing, focusing on the organizational structures needed to make sharing practical and acceptable. Following the paper's framework will enable businesses to change their behaviour and increase their sharing to meaningful levels.

Businesses need to adopt the paper's framework because increased information sharing at the organizational level creates multiplier effects across the digital ecosystem. For example, several organizations have come together through the World Economic Forum Centre for Cybersecurity to support a project called the Cybercrime Atlas. This effort combines information from widely disparate sources to develop a better picture of the cybercrime ecosystem, from malware development to distribution networks to money flows. The different "maps" or views derived from the shared information will enable the much more effective disruption of malicious cybercriminal activity. Without the underlying shared information from multiple sources, the project's analysis would not be possible.

Information sharing will never be easy. It will always require sustained resources, commitment and support. However, once businesses get into the habit, once this practice becomes the norm, we will wonder how anyone ever functioned any other way. Then, we can finally start managing our cyber risk effectively – and stop talking about cyberthreat information sharing.

Executive summary

True information sharing is foundational to closing the gap between attackers and defenders, so it is imperative to make it a reality.

> **To ensure the right level of cybersecurity, cooperation between the public and private sectors is absolutely crucial. Information Sharing and Analysis Centres create a platform for such cooperation in terms of sharing information about root causes, incidents and threats, as well as sharing experience, knowledge and analysis.**
>
> European Union Agency for Cybersecurity

This paper provides a brief discussion of three key steps towards closing the attacker-defender gap:

1. Making information sharing a C-suite prerogative
2. Managing compliance and regulatory concerns
3. Defining "sharing" on a practical level

These three steps must be implemented in concert to achieve truly productive information sharing, but it is a worthwhile endeavour given the alarming acceleration of attacks, and the relative stagnation of the progress of defenders by comparison.
In addition, this paper provides the following understandings as the foundation upon which the case for information sharing rests:

- Cyberthreats today have escalated to the point where they can pose an existential risk to a company, disrupt national/global critical infrastructure and cause the loss of life.
- For enterprises to have any chance of successfully defending themselves, they must accept and adopt a philosophy of collective defence. Cyber information sharing is at the core of any collective defence strategy.
- Information sharing is not new, and it is demonstrably not a competitive issue.
- Legal processes and emerging technical solutions exist for real and perceived regulatory and privacy challenges.
- Achieving true cyber information sharing is a business prerogative and, as with any business priority, success requires the active support and engagement of C-suite executives.

Introduction

To have any chance of successfully defending themselves, enterprises must accept and adopt a philosophy of collective defence. Cyber information sharing is at the core of any collective defence strategy.

In the spring of 1998, US President Clinton's administration was concerned with the rising tide of hostile cyber activity and the potential for that activity to harm critical infrastructure in the United States. In response, the White House issued Presidential Decision Directive 63: Critical Infrastructure Protection. Then Treasury Secretary Robert Rubin summoned the chief information security officers (CISOs) of leading financial institutions to Washington to discuss an industry response.

Work by the industry yielded one key conclusion: firms that traditionally are competitors in business need to shift their understanding of competition to the viewpoint of industry versus criminal organizations and nation-state actors. As criminal organizations are sophisticated and highly collaborative, adopting a view of collective defence is the most effective posture. Cyber information sharing is at the core of that defence. With this realization, the US Financial Services Information Sharing and Analysis Center (FS-ISAC) was born.

The idea of the ISAC has in many ways been a great success. The FS-ISAC has thousands of banks sharing information, making them more secure and more resilient. Other sectors have also benefited from information. In 2014, the FS-ISAC established its Sector Services division, which supported the development of sharing organizations based on the FS-ISAC model. The division helped build communities in legal, energy, retail and other sectors. It eventually spun out to become the non-profit Global Resilience Federation that now manages and supports 17 sharing communities. Internationally, Information Sharing and Analysis Centres (ISACs) or their equivalents can now be found around the world, working independently or with government support. As a result of their efforts, member companies are now better prepared than ever to defend themselves. But at the same time, the level of risk to industry has never been higher. In the two decades since the creation of the first ISACs, the challenges have gotten materially worse.

The world's collective reliance on services delivered in real time via the internet has exposed critical operational processes to whole new attack vectors and, in many cases, the capabilities of malicious actors have outpaced those of the defenders. In addition, these actors have adopted many nation-state style techniques and have created highly developed collaborative marketplaces for attack tools. Defenders have been left shorthanded due to skill shortages and a lack of collaboration, a weak position exacerbated by the accelerating pace of technological change.

By making information sharing a part of leadership priorities, by understanding and responding to compliance and regulatory concerns, and by more clearly defining on a practical level what sharing means, achieving an information-led approach to cybersecurity becomes an achievable and necessary business prerogative.

> **"To prevent cybercrime and reduce its impact on individuals and businesses, public-private cooperation is essential. Moving beyond reporting to real information and data sharing between companies and public agencies is the only way to identify and understand the threat and act to counter it. INTERPOL's Project Gateway offers a legal framework for private entities to share information and collaborate with the Organization. Underpinned by INTERPOL's unique global platform and range of tools, this will enable the enhanced aggregation of data and threat analysis and result in more targeted and effective operations."**
>
> Jürgen Stock, Secretary-General, International Criminal Police Organization (INTERPOL)

1 Making information sharing a C-suite prerogative

Cybersecurity cannot be addressed solely as a technical issue and must be managed as a material business risk.

At the 2015 Financial Services Roundtable featuring the largest integrated financial services companies in the United States, bank CEOs discussed systemic risks to their firms and the industry. They agreed that the impact that cyber incidents could have on operational resiliency was a top risk. The potential of a cyberattack to disrupt critical operations, putting the banks, their customers and the global financial system at risk, was material and growing. The CEOs acknowledged three key facts:

1. The adversary was getting more sophisticated and was highly collaborative.

2. Despite the significant investments being made, the banks were falling farther behind.

3. That meant the status quo was not acceptable.

A higher level of collaboration and collective defence among the banks was required, as was real engagement with government and other critical sectors to protect their firms and the global financial system.

The CEOs did not just talk about the issue; they personally engaged with government officials and put their money and staff behind a remedy, collectively funding the creation of the US Financial Systemic Analysis & Resilience Center (FSARC), now the Analysis & Resilience Center (ARC).

> **The challenges associated with cyberattacks and the financial fraud stemming from such incidents are bigger than any one institution, and this is something the financial sector must face together. We are stronger and more resilient when we work collectively to understand the evolving tactics of cyber adversaries and to deepen the layers of defence against such attacks.**
>
> Bill Nelson, President and Chief Executive Officer (2006-2018), FS-ISAC

The world has seen a significant rise in sophisticated cyber incidents over the past few years, ranging from the SolarWinds and Colonial Pipeline attacks to uncountable ransomware incidents. While aspects of the events are not new (disclosure of data, theft of money), their scale and escalation have heightened the focus on cybersecurity and operational resiliency by corporate leaders in every sector of the economy, members of the media and government officials.

The silver lining to the increased cyberthreat is a growing understanding that a bad cyber day can pose an existential threat to a company. Cybersecurity cannot be addressed solely as a technical issue and must be managed as a material business risk. This realization has amplified the focus of management teams and boards of directors. This combination of increased focus and collective vulnerability offers an opportunity for CISOs to engage their C-suites to seek their active support to enhance collaboration, better defend and protect organizations against these threats, and improve the security and resiliency of the collective ecosystem.

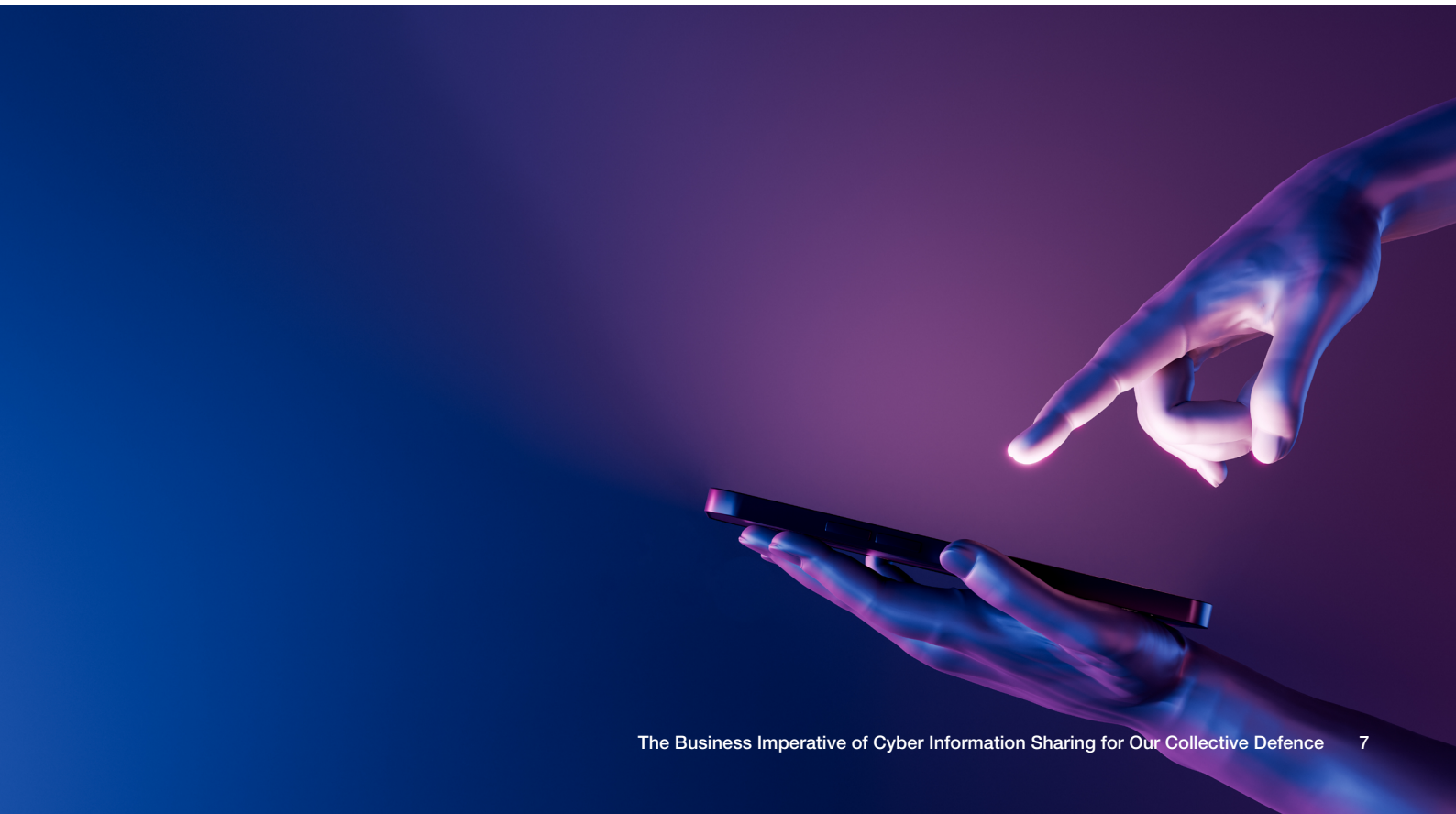
One specific action a CISO can take to better engage with senior executives is to schedule a cyberthreat information briefing for their C-suite executives and board of directors with their relevant law enforcement/governmental agency. President Biden's 12 May 2021 Executive Order on Improving the Nation's Cybersecurity starts with the need for better cyber information sharing.

The European Union Agency for Cybersecurity (ENISA) states on its website that "European legislation like the NIS Directive and the Cybersecurity Act nourish the creation of sectoral ISACs and public-private partnerships within the EU". The EU's Digital Operational Resilience Act also proposes to specifically develop information and intelligence sharing protocols.

The private sector should drive engagement in information collaboration. This can seem unnatural in competition-driven businesses, but history has demonstrated that cybersecurity is neither a competitive nor an anticompetitive issue. Mutual success requires a willingness to work together. An active interest in collaborating operationally is necessary to share observations, lessons learned, best practices and intelligence in order to protect the enterprise, its clients and the ecosystem.

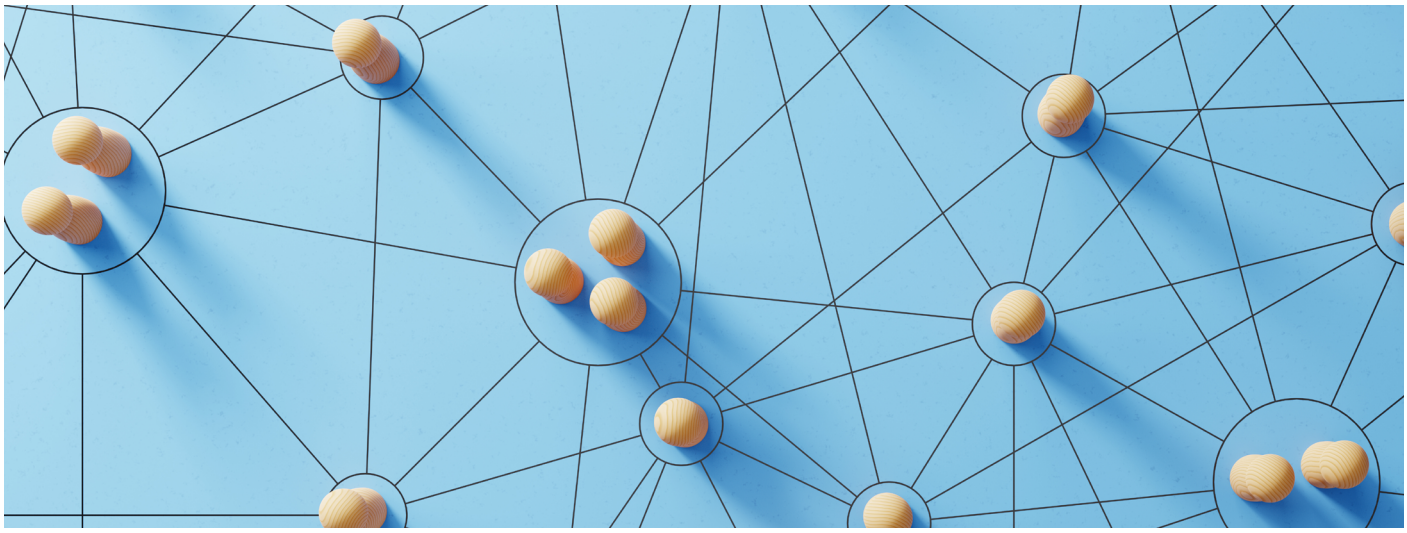
As a result, when company leaders make sharing a real priority, it has a chance to succeed. In contrast, information sharing efforts often wither without sustained support from the top. Effective sharing requires continuous support; the CEO and other senior company officials must make cyberthreat information sharing an ongoing priority for it to be impactful and sustainable.

> **A platform of trust and communication to facilitate information sharing among sectors and businesses is necessary to share actionable insights with other stakeholders for situational awareness, and to detect and respond to cyberthreats promptly.**
>
> Cyber Security Agency of Singapore



2 Managing compliance and regulatory concerns

Sharing agreed-upon information is certainly more beneficial than harmful to companies.



Despite the importance of sharing, neither the public sector nor the private sector is acting quickly enough. What are some of the factors impeding progress? One is that it may be difficult to shift from a competitive to a collective perspective; safeguarding company information is ingrained to such an extent as the status quo that sharing may seem antithetical to good business practice. With the proper C-suite support, however, this barrier can be overcome.

Other barriers raised often relate to the protection of intellectual property and proprietary information, and the perceived legal/regulatory/compliance barriers to sharing. Yet, organizations can address confidentiality and balance the protection of proprietary information with tried and tested sharing protocols that do not require businesses to divulge sensitive material.

Given these challenges, CISOs must work with their legal and compliance partners to help their organizations overcome the barriers and improve information sharing.

Legal counsels can work with CISOs on cyber information sharing in the following key areas:

Defining the terms and conditions
In the absence of governmental directives on cybersecurity information sharing, it is up to corporate legal departments to determine the "terms and conditions" when entering into collaborative agreements. Some of these rights and obligations may include:

- Ensuring rules of information sharing that account for data residency and cross-border issues
- Safeguarding confidentiality, through the use of non-disclosure agreements
- Complying with existing regulatory requirements
- Defining who receives the data and what they are allowed to do with it
- Determining the most secure way of providing cross-company data

The type of information that is shared is crucial to offsetting this issue. If it is nuanced, actionable and readily available to security teams, and particularly when the collaboration with law enforcement is

strong, sharing agreed-upon information is certainly more beneficial than harmful to companies.

Terms of sharing should be written into the original contracts when forming a collaborative network. Where possible, leveraging existing agreements such as those with the various ISACs and the UK's Cyber Defence Alliance (CDA), among others, is advisable.

Ideally, governments would provide the main guidance on these processes. However, in the absence of clear regulation, creating rules, up-front terms and other best practices will help facilitate sharing.

Building a trust framework

Although contracts can offer a roadmap on how to proceed, trust plays a crucial role in the success of any collaborative effort.

It is possible to build trust within a coalition by setting standards and rules of behaviour that every partner can agree upon. One example is the Traffic Light Protocol, a set of designations created to facilitate greater information sharing, adopted by most ISACs. To be useful, a minimum requirement may be necessary to ensure that companies are not gaining from a collaborative effort without contributing their own resources.

Recommendations include laying out clear ground rules for confidentiality and anonymizing data to protect the privacy of individuals. Leveraging emerging technology capabilities where possible to protect personally identifiable information (PII) is also advised.

At the same time, it is imperative to acknowledge that not all data is highly sensitive PII. A clear data identification system can help to alleviate this pressure.

Although information sharing entails compliance costs, better security will benefit every business in the long term. Private-sector-led cross-sector information sharing should create an impetus for clearer legislation on sharing across borders with data residency and sovereignty implications. Expanding cooperation benefits everyone, and a code of best practices builds a stronger coalition to protect collective security. Until governing bodies pass legislation, companies must continue to depend on their legal departments to create a path forward, based on established precedent.

3 Defining “sharing” on a practical level

It is essential to rethink how organizations engage in collaboration and the requirements to make it successful.

Even if an organization follows all the above-mentioned recommendations – recognizing the value of information sharing, obtaining its CEO’s approval and resolving the General Counsel’s questions – making information sharing work can still prove challenging.

Industry and government partners that have previously discussed partnerships in cybersecurity have primarily focused on information sharing as a transaction. However, the sharing needs to be continuous and perpetual – active during both heightened and decreased threat periods. To benefit all those involved, collaboration should occur in trusted physical and virtual environments and should be easier and more streamlined, with clarity on entry points as well as roles and responsibilities.

By collaborating within a known and trusted community, “circles of trust” are established. As described by Chris Johnson et al. in NIST Special Publication 800-150 entitled “Guide to Cyber Threat Information Sharing”, “organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face.” Using this knowledge allows an organization to make better informed decisions, and create better threat detection techniques and risk mitigation strategies. “By correlating and analyzing cyber threat information from multiple sources, an organization can also enrich existing information and make it more actionable.”

Four steps can shift true information sharing from concept to reality:

- Preparing the company
- Identifying partners
- Understanding what to share
- Protecting privacy

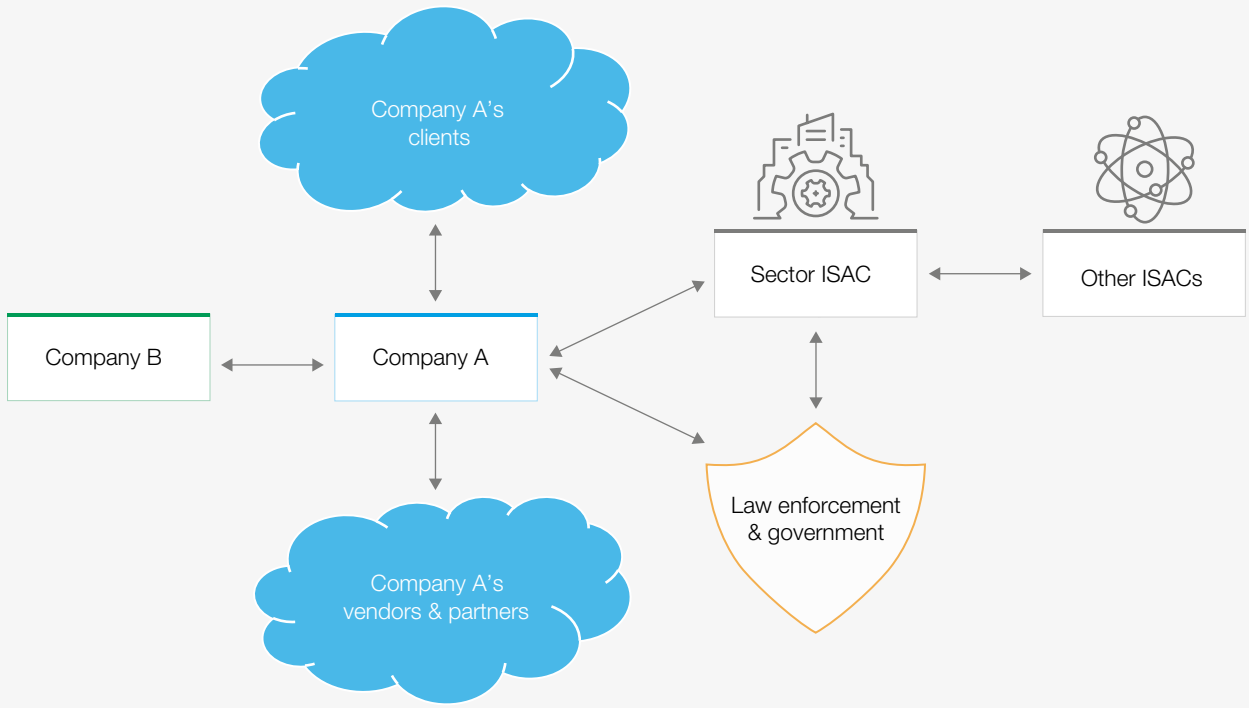
Preparing the company

- Determining information requirements
  - The challenge stems from the sheer volume of information. To sort through the ocean of intelligence, organizations need to determine their information requirements based on the cybersecurity decisions their company needs to make.
- Selecting the right type of information
  - Once a business understands its cybersecurity use cases, it then must select the information that supports those use cases.
  - Many types of information exist, ranging from technical indicators to threat actor profiles to defensive measures and best practices.
- Integrating security actions in business activities
  - This step involves integrating the information in the firm's security and business decisions.
- Ensuring sustainability
  - Weaving information sharing into the day-to-day activities of cybersecurity staff and providing regular funding are critical for success.

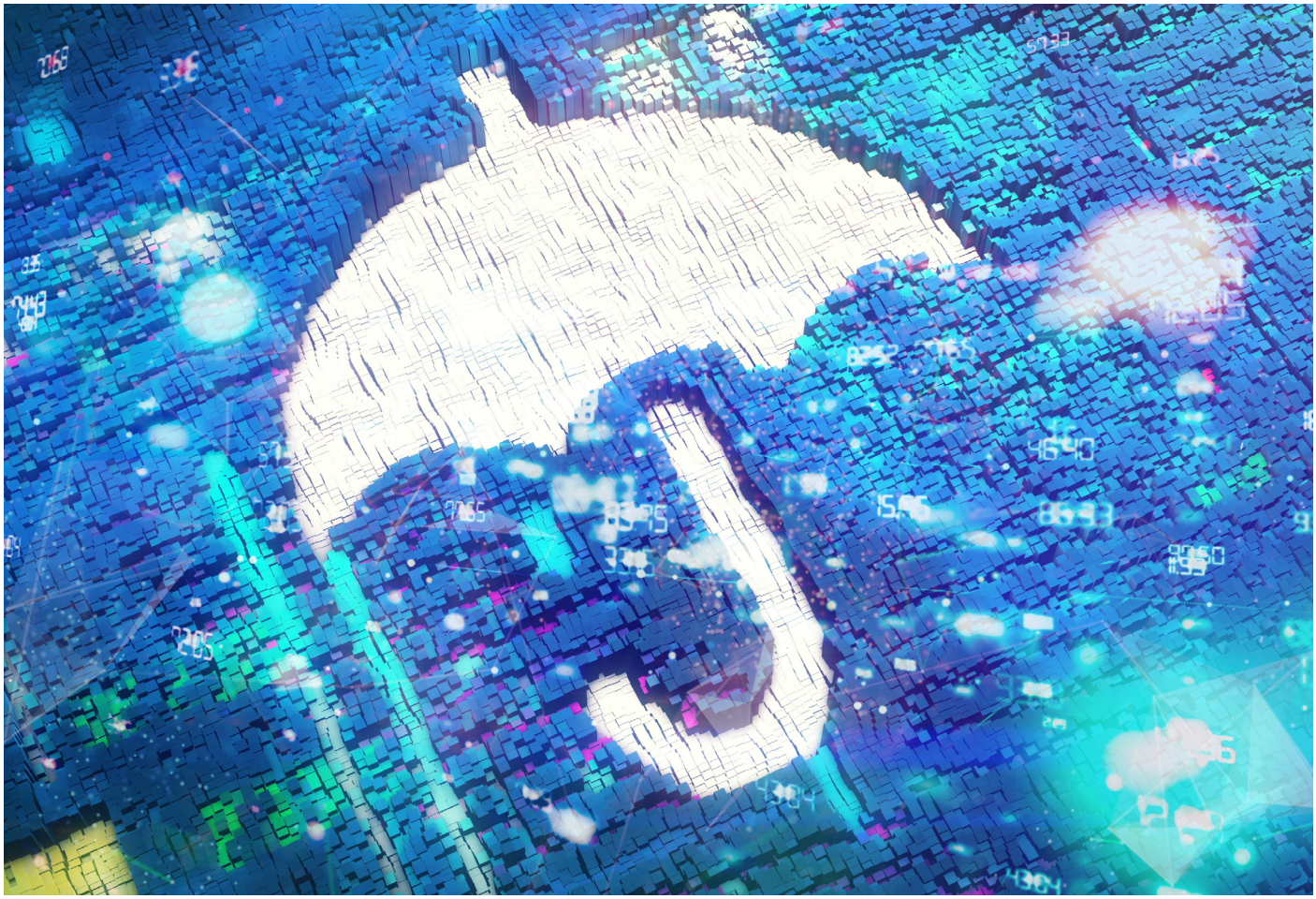
Identifying partners

- All organizations wish to receive intelligence but for there to be any relevant information to receive, someone has to share it in the first place. As with the information consumed, the information an organization shares back and how it does so depend on its situation.
- Sharing back does not mean an organization must share everything, but it does require sharing to be bidirectional.
- Sharing networks need to support multiple types of sharing partnerships.
- The fastest way to achieve sharing is to build on top of an existing network whenever possible.
- Sharing is at its most impactful when it is built on circles of trust. Within the ISACs, circles of trust are often formed between the leaders of the security operations and intelligence teams from the various participating companies.
- One key recommendation is to think about circles of trust occurring at various layers of an organization, going both deeper within the organization but also, and more critically, higher within it so that CISOs and CIOs are also talking to each other.

FIGURE **A sample sharing ecosystem**



ISAC = Information Sharing and Analysis Centre
Source: Global Resilience Federation



Understanding what to share

- The goals of sharing must not be arbitrary. They should be determined by well-defined use cases that fall into one of the following categories:
  - Protecting the firm's ability to operate safely
  - Protecting the firm's clients
  - Protecting the safety and soundness of the "system"
  - Protecting the nation's critical infrastructure
- Often, the perfect is the enemy of the good, as organizations assume that because some information is too sensitive to share, they cannot share anything useful.
  - Some information is almost always better than no information.
  - Knowing what may prove useful to another company is usually impossible, so erring on the side of sharing makes sense.

Protecting privacy

- A key consideration when sharing is how to share while complying with the various international privacy regimes.
- A new broad range of technologies called "privacy-enhancing technologies" (PETs) has emerged to address this challenge.
  - PETs enable organizations to share data while preserving privacy, security and regulatory compliance.
- A variety of PETs are available today, including homomorphic encryption, secure multiparty computation and differential privacy, each of which offers solutions to different collaboration challenges.
  - In particular, homomorphic encryption has become popular in organizations that endeavour to collaborate with their ecosystem on sensitive data while protecting their business interests and complying with data privacy regulations.

Conclusion

The escalating cyberthreat environment presents a risk of operational disruption to every enterprise today. At the extreme, attacks can pose an existential threat to a company or, worse, can lead to the loss of life.

To have any chance of successfully defending themselves, enterprises must accept and adopt a core philosophy of collective defence; true cyber information sharing is at the centre of a collective defence strategy.

Information sharing is vitally important for an effective approach to cybersecurity. In the United States, for example, the Cybersecurity & Infrastructure Security Agency and, in the EU, ENISA both have identified information sharing as essential to improving the world's cybersecurity risk posture.

As with any business priority, success relies on the active support and engagement of the C-suite, and traditional reluctance stemming from competitive, regulatory compliance and privacy perspectives must be put aside.

Achieving true cyber information sharing is a business prerogative that requires an appetite for collaboration and swift action by all organizations.

> **Cyber is the ultimate team sport, and we need to create an environment where the challenges experienced by one company lead to the benefit of many companies. Intelligence sharing is a critical component in our ability to achieve that goal."**
>
> Admiral Michael Rogers (Ret), Director, US National Security Agency (2014-2018), and Head, US Cyber Command (2014-2018)

Contributors

World Economic Forum

Gretchen Bueermann
Research and Analysis Specialist, Centre for Cybersecurity

Tal Goldstein
Head of Strategy, Centre for Cybersecurity

Partner organizations

Global Resilience Federation

Charles Blauner
Special Adviser

Mark Orsi
Chief Executive Officer

Cyber Threat Alliance

Michael Daniel
President and Chief Executive Officer

Acknowledgements

Partnership against Cybercrime

Keith Agisim
Chief IP Counsel, Bank of America, USA

Philipp Amann
Head, Strategy, European Cybercrime Centre, Europol, Netherlands

Shilpa Bratt
Director, Shared Services, Microsoft Digital Crimes Unit (DCU), Microsoft, USA

Jaime Calvo
Head, Legal Counsel for Cybersecurity, Banco Santander, Spain

Michael Daniel
President and Chief Executive Officer, Cyber Threat Alliance, USA

Craig Froelich
Chief Information Security Officer, Bank of America, USA

Michael Garcia
Senior Policy Adviser, Third Way, USA

Josey George
Distinguished Member of Technical Staff, Wipro, India

James Gill
Global Head, Cyber Threat Response, Banco Santander, Spain

Oliver Gower
Group Director, Cyber Forensics, Investigation and Intelligence, Banco Santander, Spain

Thomas Harvey
Global Head, Cyber Response and Intelligence, Banco Santander, Spain

John Holmes
Chief Legal Officer, Forcepoint, USA

Jeanette Jarvis
Chief Recruitment and Marketing Officer, Cyber Threat Alliance, USA

Fiona Johnson
Manager, National Cyber Crime Unit Partnerships, National Crime Agency, United Kingdom

Wookyung Jung
Cyber Policy Analyst, International Criminal Police Organization (INTERPOL), Lyon

Mary Kavaney
Chief Legal and Administrative Officer, Global Cyber Alliance, USA

Ilene Klein
Global Cybersecurity Coordinator, Cybercrime Support Network, USA

Derek Manky
Chief Security Strategist and Vice-President, Global Threat Intelligence, Fortinet, USA

Jaap van Oss
Partnership and Engagement, EMEA Cyber Intelligence Center (CIC), Citi, USA

Cláudia Pina
Member, Cybercrime Team, Eurojust, Netherlands

Kristin Royster
Senior Vice-President, Global Information Security, Bank of America, USA

Michael G. Shanahan
Unit Chief, Cyber Directorate, Federal Bureau of Investigation, USA

Don Spies
Director, Strategic Initiatives, Chainalysis, USA

René J. Steiner
Administrator, European Commission, Belgium

Nicholas Tuppen
Lead, Global Cyber Crime Partnerships, Bank of America, USA

Juan Antonio Velasco
Cybersecurity Analyst, Global Threat Response, Banco Santander, Spain

Rob Wainwright
Partner, Deloitte, Netherlands

Lindsay Whyte
Regional Director, Constella Intelligence, Spain

Steven Wilson
Chief Executive Officer, Cyber Defence Alliance, United Kingdom

Keong Min Yoon
Counsel, World Bank, Washington DC

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org