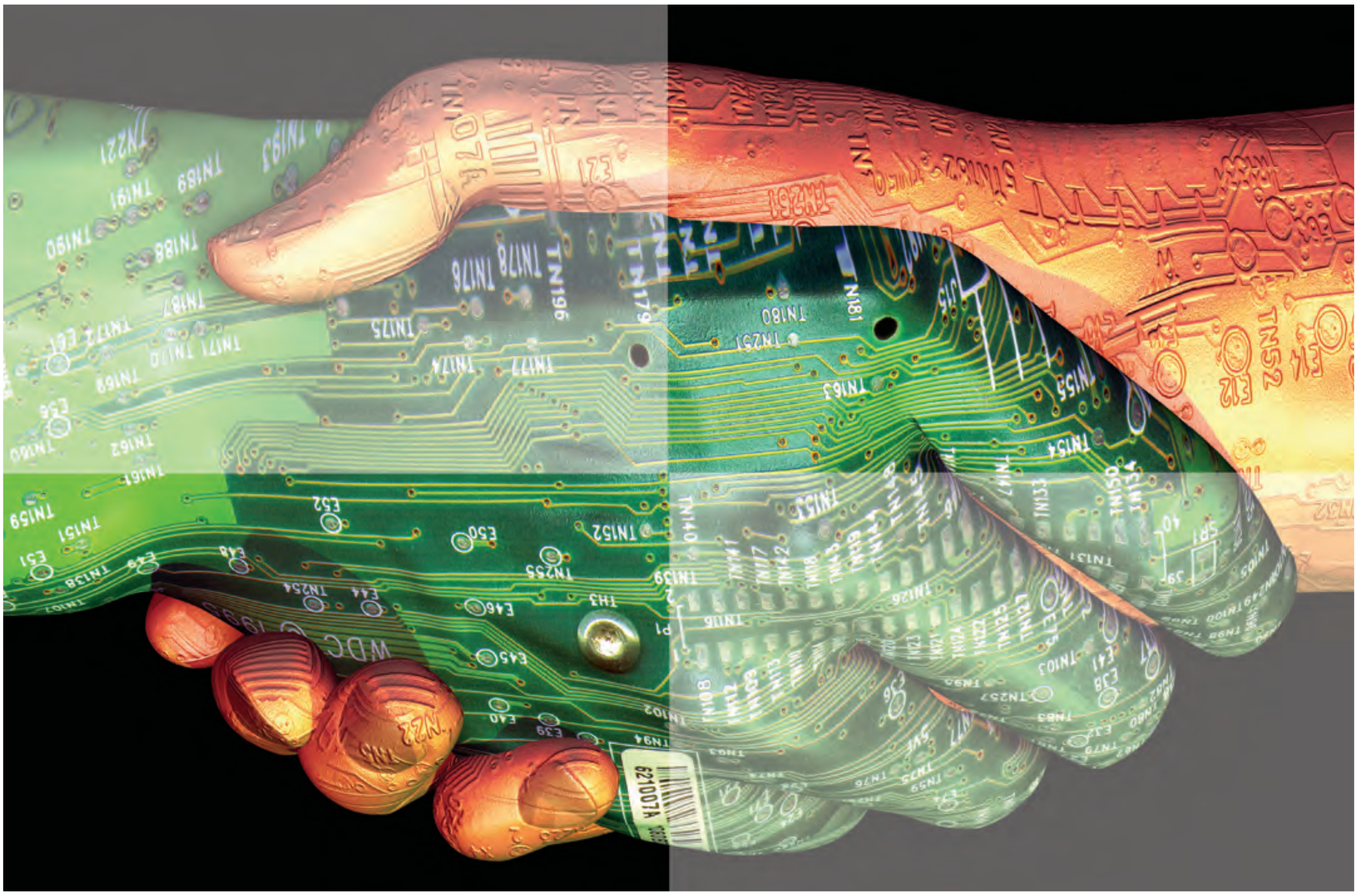
WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Risk and Responsibility in a Hyperconnected World
Pathways to Global Cyber Resilience

Prepared in collaboration with Deloitte

June 2012



Contents

5 **Introduction**

6 **Executive Summary**

8 **Section 1: The Changing Landscape**

- 9 The Hyperconnected World
- 12 Risk and Responsibility
- 13 Cyber Risk Framework

15 **Section 2: Individual Action – Collective Gain**

- 16 Partnering for Cyber Resilience
- 18 Cyber Resilience as an Enabling Capability

21 **Section 3: Collective Action – Individual Gain**

- 22 Economics of Cyber Security
- 26 Information Sharing
- 31 Case Studies
- 35 Conclusion

38 **Definitions**

41 **Appendix**

43 **Endnotes**

45 **Acknowledgements**

47 **Contacts**

Introduction

Throughout the course of 2011, the World Economic Forum developed a multistakeholder project to identify and address emerging global systemic risks arising from the increasing connectivity of people, processes and objects. In particular, the project has focused on cyber security, with the objective of working with the private sector across multiple industries and governments across multiple regions to identify pathways to a more secure shared online environment. Dedicated workshops took place across Asia, Europe and the United States.

An initial period of discovery provided the context, direction and initial tools for dialogue:

- Nature of the Problem – Increasing connectivity makes us increasingly interdependent. Cyberspace is a global commons and we all have a role in protecting it. Success in complex networks requires new ways of thinking
- Strategic Approach – Provide leaders with simple actionable steps; secure commitment to simple steps to provide a platform for trusted dialogue, especially between private and public actors
- Common Framework – A common cyber risk landscape was developed to provide strategic overview of issues

As a result of the ongoing efforts of the Risk & Responsibility in a Hyperconnected World project's stakeholders, the World Economic Forum launched the community-led Partnership for Cyber Resilience initiative at the Annual Meeting 2012 in Davos, Switzerland.

This initiative offers a common set of principles for leadership, raising business standards and shifting mindsets based on just securing perimeters to a focus on interdependence and resilience. By committing to these principles, chief executives and executives in a similar capacity demonstrate leadership, accountability and best practice corporate governance in a digital world. The principles are supported by a set of optional practical tools for CEOs and other executives.

The organizations taking part in this initiative show themselves to be trusted business partners and legitimate voices in the policy debate around cyber security and related issues. In 2012, the Risk and Responsibility in a Hyperconnected World project will host a number of public sector-focused workshops to provide signatory organizations a platform for this debate.

While the Partnership for Cyber Resilience initiative is relevant to public sector organizations in their operational capacity (they are also actors in the ecosystem), it does not speak to the special role that government has in providing the environment in which organizations operate.

The highly networked nature of cyberspace presents policy-makers with unique challenges. In particular, there is growing awareness that policies designed as a solution to one particular problem can frequently have unintended consequences elsewhere, e.g. on privacy, innovation or even existing and commonly accepted business practices.

A striking outcome from the regional workshops was the high degree of alignment on the overarching goals that businesses and governments wish to achieve. However, this was matched by recognition of significant regional and national differences in capabilities to deal with cyber threats and cyber crimes. Cultural differences in norms and values, and the debates these engender, will continue for some time. However, there is an opportunity to harmonize on a core set of non-prescriptive capabilities, such as in the criminal justice chain, to deliver both immediate gains and a platform for continued dialogue.

Executive Summary

As private and public sector actors take steps towards greater accountability and capabilities, discussions on collaboration across sectors and regions can be undertaken with greater trust, confidence and experience.

Scott David, Executive Director of the Law, Technology & Arts Group, University of Washington Law School; and Raymond Stanton, Global Head of Business Continuity, Security and Governance, BT Group

This document is structured to capture some of the emerging and leading thoughts on the current cyber security debate.

Section 1 describes some of the relevant attributes of the "hyperconnected world" as a complex network. In particular, it highlights the changing nature of relationships as driving a great deal of uncertainty over roles and responsibilities. A two-step approach to greater clarity and confidence is proposed:

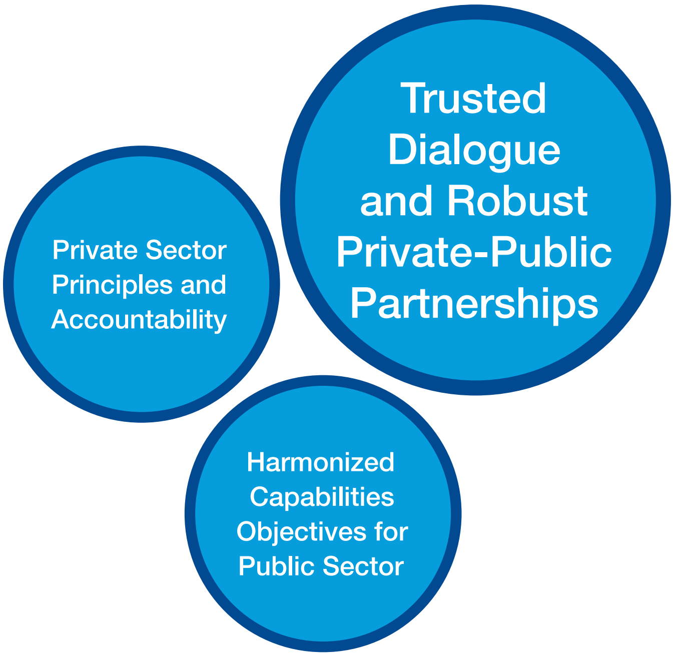
- Identify and promote individual actions that have an effect on the overall environment (e.g. an analogy is often drawn with basic hygiene practices, such as washing your hands to stop the spread of germs or viruses)
- Actors who have committed to these practices can engage in a dialogue to work through new ways of working together; mutual trust provides a platform for collaboration

Section 2 provides an overview of the Partnership for Cyber Resilience initiative, including the Principles for Cyber Resilience. It highlights why the Principles are relevant and should be taken up by the executive leader of organizations across all industries and sectors. It also addresses an emerging discussion about cyber resilience and national competitiveness. While steps can be taken to increase resilience by both companies and governments, it is clear that collaboration and coordination is required.

Section 3 looks at questions of coordination. Functioning markets are a powerful tool for allocating resources for maximum social gain. However, markets need supporting institutions (e.g. property law and contract law) in order to operate, thus market failures may require specific responses to achieve desired outcomes (e.g. environmental pollution constraints). How does the challenge of securing cyberspace look through this lens? An example of those challenges is the sharing of information among stakeholders. Information access is an important feature of equitable markets and information sharing is a common focus for cross-industry, cross-sectoral and transnational cooperation. However, it can mean different things to different people and some challenges and barriers still prevent stakeholders from fully reaping the benefits of information sharing. A simple analysis of the dimensions of information sharing is provided and applied to two case studies.

Discussions and workshops held as part of the Risk and Responsibility in a Hyperconnected World project over the last year have led to the following recommendations:

- **For the private sector:**
  - Join the Partnering for Cyber Resilience initiative; commit to the Principles
  - Develop a pervasive culture of cyber awareness and resilience
  - Commit to responsibility and accountability for developing the organization’s level of cyber resilience
  - Promote the spread of best practices throughout supply chain
  - Engage in policy debate, and where possible, align under common core principles and commitments as a first step towards harmonizing policy needs
- **For the public sector:**
  - Work towards a flexible, but harmonized criminal justice capabilities framework
  - Engage private sector and adjacent policy domain experts to identify potential unintended consequences of policy development in advance
  - Ensure individual protections and foreign jurisdiction counterparts to share lessons learned and improve harmonization
  - For public agencies: join the Partnering for Cyber Resilience initiative; commit to the Principles


Trusted Dialogue and Robust Private-Public Partnerships
Private Sector Principles and Accountability
Harmonized Capabilities Objectives for Public Sector

- **For the private and public sectors together:**
  - Commit to develop robust and sustainable public-private partnerships for a resilient cyber environment, based on clear and mutually agreed assignment of roles and responsibilities and the principle of accountability
  - Explore the need for the development of a cyber risk market
- **For academia:**
  - Promote the concept of economics of cyber security to non-specialist fields
  - Advance research on information sharing and the link between cyber resilience and national competitiveness

In the second year of the Risk and Responsibility in a Hyperconnected World project, the World Economic Forum will develop a tailored, capabilities-based set of guidelines for the basic legal and criminal justice components that governments should put in place to improve cyber resilience. The project will seek interaction with government representatives, both in policy development and policy enforcement communities, academics and business representatives in a series of workshops and interviews. This will contribute to developing guidelines for policy and criminal justice communities, and subsequently to seek support for this new initiative.

The interim results will be presented during the World Economic Forum Annual Meeting of New Champions 2012 in Tianjin, People’s Republic of China on 11-13 September.

Section 1: The Changing Landscape

The Hyperconnected World

Being always "connected" is the new normal. Such a level of interconnectedness presents unique and substantial risks, but also opportunities. As new business models develop and non-traditional sectors are integrated into the hyperconnected world, the question of responsibility and ownership becomes critical for the viability and stability of the entire digital ecosystem. Building a common understanding of rights and responsibilities therefore becomes essential.

Hamadoun I. Touré, Secretary-General, International Telecommunication Union (ITU)

Information and communication technologies are at the centre of a rapid expansion of physical, social and virtual networks, connecting objects, people and processes in new ways and on an unprecedented scale. There is increasing awareness that we are rapidly entering a world in which everyone and everything is, will be or can be connected.

Over 2 billion people are now connected to the Internet, and this number is set to increase significantly with the advance of the "Internet of things,"[1] in which a wide range of networks, devices, appliances and objects are to be connected. In addition, the total data traffic generated by mobile devices is projected to surpass that of wired devices by 2015.[2] Some have predicted that by 2020 there will be over 50 billion Internet-connected devices.[3]

Being connected has become the new normal across so many aspects of our lives, driving huge change across the worlds of business, government, civil society and our daily lives. In fact, information and communication networks have become a fundamental part of a nation's infrastructure, needed for economic stability and growth. Such networks lead to increased productivity, business growth and job creation.[4] However, there is a growing sense that the changes are only beginning, and perhaps more importantly, that it may be hard to fully understand the breadth and depth of opportunities and risks which this connectivity brings.

Hyperconnectivity does not just allow us to do things more efficiently; it transforms how we do things and even what can be done. From smart grids and e-health to embedded sensor networks, technology is enabling innovative collaboration and new types of partnerships, particularly between businesses, governments and individuals.

However, this can bring about both benefits and harms, social and economic alike. On one hand, first responders to the Chilean earthquake in 2012 were connected via a volunteer mapping platform with real-time needs communicated through texts from victims on the ground.[5] On the other hand, cyber crime is estimated at up to US $ 1 trillion annually.[6]

The Internet of Things

As defined in the World Economic Forum's ***Global Information Technology Report 2012***, hyperconnectivity includes not only people-to-people formats (as individuals and as members of groups, and using a vast array of media), but also communication between people and machines, and between machines themselves without any direct human involvement.[7]

Today, so many physical objects and processes are being connected. Everything from business processes to critical infrastructure, cars, planes, household appliances, pacemakers – all are in some way connected to networks. This allows for huge social and economic gains. The data that this connectivity produces can result in genuine new knowledge of the world and trends.

But there is a downside. The risk of this "connectivity of things" has been described by Rod Beckstrom in terms of "laws":

- Law 1: Everything that is connected to the Internet can be hacked
- Law 2: Everything is being connected to the Internet
- Law 3: Everything else follows from the first two laws

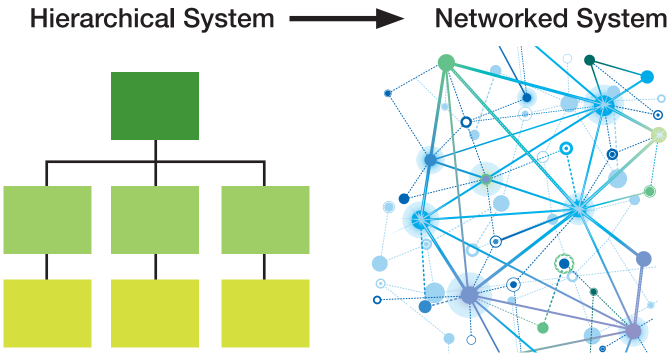
Less Clear Boundaries

The concept of de-perimeterization has emerged in the last decade as the borders between the internal and external networks are becoming less clear. Employees increasingly use their own devices for work purposes; partners, contractors and customers share access to networks and cloud-based services continue to enjoy rapid growth. Security technologist and author Bruce Schneier highlights the notion that modern networks are more like cities, dynamic and complex entities with many different boundaries within them. The access, authorization and trust relationships are even more complicated.[8] As such, thinking about security in terms of building bigger walls (firewalls and anti-virus software), while still necessary, is not sufficient. A holistic approach to cyber risk management – across the organization, its network and the larger ecosystem – is required.

From Centralized Authority to Distributed Accountability

Networks allow for point-to-point interactions, which spread power broadly across its participants. Whether those participants are consuming digital goods (e.g. music, books), rating physical products or services (e.g. retail, travel) or exercising their political voice, social and institutional structures need to adapt.

There are many examples where today's social structures are transforming from a centralized, hierarchical structure to a decentralized networked system composed of multiple nodes, all able to interact with each other. The move away from "command and control" social structures make decision-making much more challenging for at least two reasons: unilateral decisions based on authority have less influence, and the number of complex interdependencies can mean that steps taken to solve a problem in one domain can result in unintended consequences elsewhere.



From a risk perspective, the bottom-up, distributed nature of networks also poses new challenges. On the threat side of the equation, the asymmetry of power between the individual and the state is inverted, and malevolent actors can recruit, coordinate and inflict harm across the whole network. Highly connected networks are typically robust to random failures, but are vulnerable to targeted attacks. Furthermore, a recognized risk in networked environments is that of cascading failure, exemplified by "Operation Blackout" by hacking collective Anonymous,[9] which intended to use this networked characteristic of the Internet to disrupt availability.

On the response side, a shared networked environment makes us more interdependent on each other.

Increasing dependence on connectivity for the normal functioning of society makes the protection of connectivity a critical issue for all; it is a shared resource, like clean air or water. No one organization can resolve the issue by itself; a collaborative, multistakeholder approach must be taken. Even competitors in a given industry must become partners in the effort to ensure a stable and trusted environment.

The Changing Nature of Relationships

- **State – Citizen:** The empowered citizen has been the focus of much media attention, as a result of improved transparency and coordination. At the same time, the amount of citizen information governments possess has never been higher.
- **Enterprise – Consumer:** The empowered consumer drives change across business models and practices, while corporations are the trustees of vast amounts of personal customer data.
- **Enterprise – Enterprise & Government:** Companies are discovering opportunities to collaborate across industries to bring new value propositions, from smart grids to smart cities and the connected car. These propositions often have social value to governments or require new laws.
- **Enterprise – Enterprise:** Competitors in the same industry are beginning to share critical cyber risk and threat information with each other in ways that would have seemed inconceivable only five years ago.
- **Government – Government:** Hyperconnectivity does not respect borders or boundaries, requiring improved transnational and cross-sectoral coordination; the rate of change in the nature of threats renders current policy-making practices and timeframes inadequate, at least in the case of threat or technology specific policy

The changes in how actors can interact with each other – be they governments, citizens-consumers or enterprises – not only means that often the "old rules" do not apply, but it also means that the type of rules and the way in which rules are made, might also need to be re-examined.

Risk and Responsibility

Hyperconnectivity is allowing new types of interactions between actors or nodes in our society and economy, demanding a renewed examination of roles and responsibilities.

As new behaviours and models are emerging, individual and organizations are faced with the need to adapt to new ways of thinking and effect change in a new environment. The approach is two-fold:

- *Identify new behaviours for individual nodes:* This process requires working on developing the networking effects by aligning individual behaviours.
- *Reconsider the terms of the contracts between the nodes:* Once individual behaviours are aligned, the terms of the social, commercial and legal contracts between individuals need to be re-examined and adjusted.

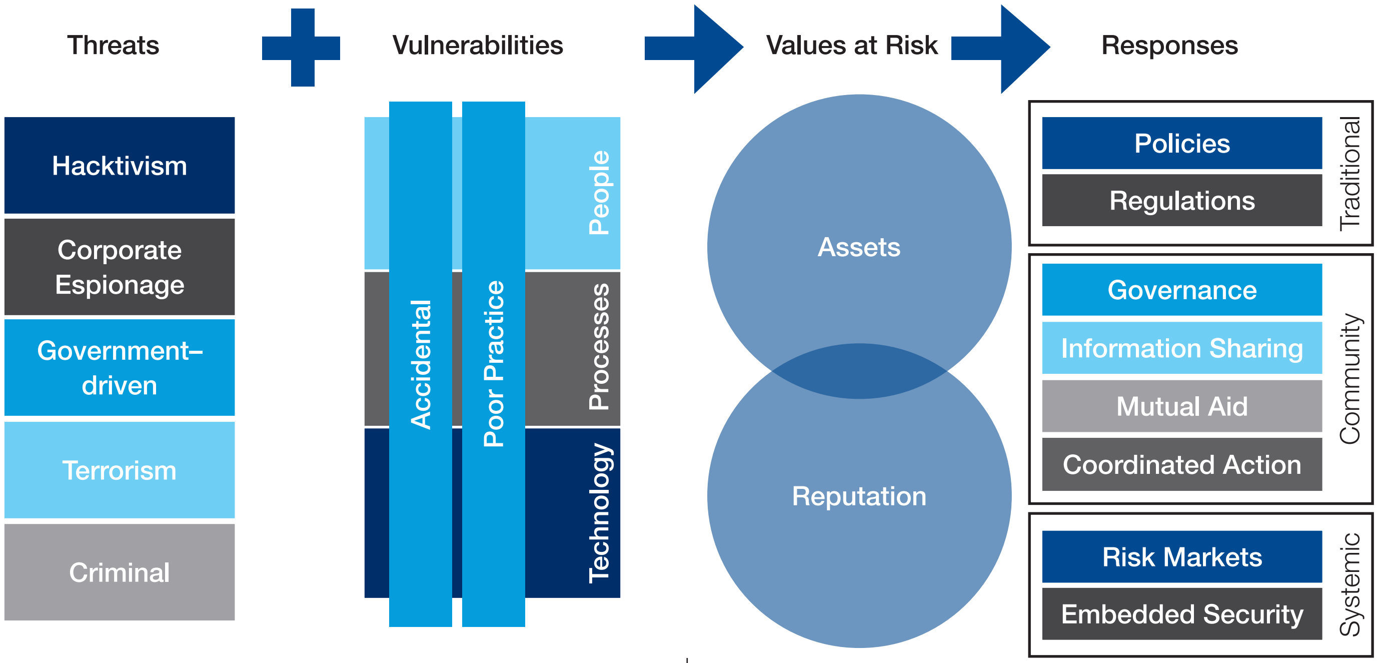
By developing the Partnering for Cyber Resilience initiative, the World Economic Forum intends to help any organization in its operational capacity to improve its internal cyber capabilities and resilience and become a trusted node in the network.

A new phase of the initiative is now being developed to help public sector organizations in their decision-making capacity to enforce policy in the hyperconnected world. The objective is to create a tailored, capabilities-based set of guidelines or principles for the basic legal and criminal justice components that the public policy and criminal justice communities can use to reduce cyber crime at a national level, and to benefit them in developing and enforcing policy in the hyperconnected world.

Both parts of the initiative are helping each node of the network to focus on similar objectives and adopt a common approach to address the challenges emerging from the hyperconnected world. The three issues discussed in this report – cyber resilience as an enabling capability, the economics of cyber security and information sharing – focus on the interactions between the nodes and examine the new terms of the contract that needs to be identified to adapt relationships to this new environment.

Ian Livingston, Chief Executive Officer, BT Group

Cyber Risk Framework



Initial insights from the World Economic Forum's Risk and Responsibility in a Hyperconnected World project highlighted the need for stakeholders to adopt a common understanding of cyber risk in a hyperconnected world. Stakeholders participating in the project have developed a risk framework to help further the dialogue.

Threats

Cyber threats are as numerous as they are complex. The tools malefactors use, the objectives they are seeking or the authors that are behind them vary from case to case. The risk framework categorizes threats into five major categories: hacktivism, criminal, government-driven, terrorism and corporate espionage. These categories are not intended to be mutually exclusive; one person's hacktivism may be another's cyber-terrorism. Rather, the framework intends to identify the major existing threats in order to define the most adequate and efficient approach to addressing the range of risks they present.

Recent cyber attacks by hacktivist groups against business targets have caught the world's attention. These loose, self-forming online coalitions have directed their efforts towards hacking, conducting distributed denial of service (DDoS) attacks, and defacing websites of businesses or government entities for purposes of political or policy protest. Cyber criminals are reaping rewards from the theft of identities, intellectual property and funds. The risk of prosecution or other consequences has been low, making the risk-return trade-off extremely favourable when compared to other types of crime.

In 2010, the Stuxnet worm raised the bar on cyber attacks as it was a direct attack on critical infrastructure. The attack has been widely debated, but the consensus appears to be that it was a government-driven attack.[10] Since its release, some of its code has been used as a blueprint for other malefactors to develop future cyber weapons. While the very targeted Stuxnet code was primarily intended to disable machinery, the recent Flame malware indicates that there are actors willing and able to design extensive, highly complex and sophisticated code to gather and delete vast amounts of information.

Global terror organizations have also started to conduct operations in cyberspace, primarily for recruiting and command-and-control activities. While the number of cyber terrorist attacks has been quite small so far, it is anticipated to grow in the future.[11] Additionally, cyberspace offers a lucrative marketplace for sensitive corporate information and intellectual property.

Vulnerabilities

A cyber attack usually achieves its objectives through the exploitation of one or more vulnerabilities in technology, process or human action. Cyber events can be the result of accidents, in many cases through the unwitting action of employees or business partners who lose storage media or otherwise expose data. Cyber vulnerability may also be the result of exploitation of poor practices, such as inadequate patching of known vulnerabilities, or insecure data transmission and storage. Therefore, cyber threat education and awareness – particularly prevention – are crucial elements for improving cyber resilience.

Values at Risk

Cyber threats have a wide range of potential impacts for governments, companies and individuals: denial of service, data exposure, disinformation, reputation damage and loss of trust. These damages may be summarized into two broad categories: assets and reputation. Assets in this context includes the integrity, availability and security of data, networks and connected devices, which by extension includes business continuity and the associated cost of an operational shut down or slow down. It also includes critical infrastructure and longer term damage related to loss of competitive position where intellectual property is compromised. Reputation in this context refers to the ongoing standing and trust of the organization, with stakeholders such as customers, constituents, business partners, owners, stockholders and employees. Reputational damage might result in a loss of customers and sales, difficulties in engaging business partners, loss of investment or financing, and in the case of government entities, political damage to government officials and programmes as well as a decrease of citizens' confidence.

Responses

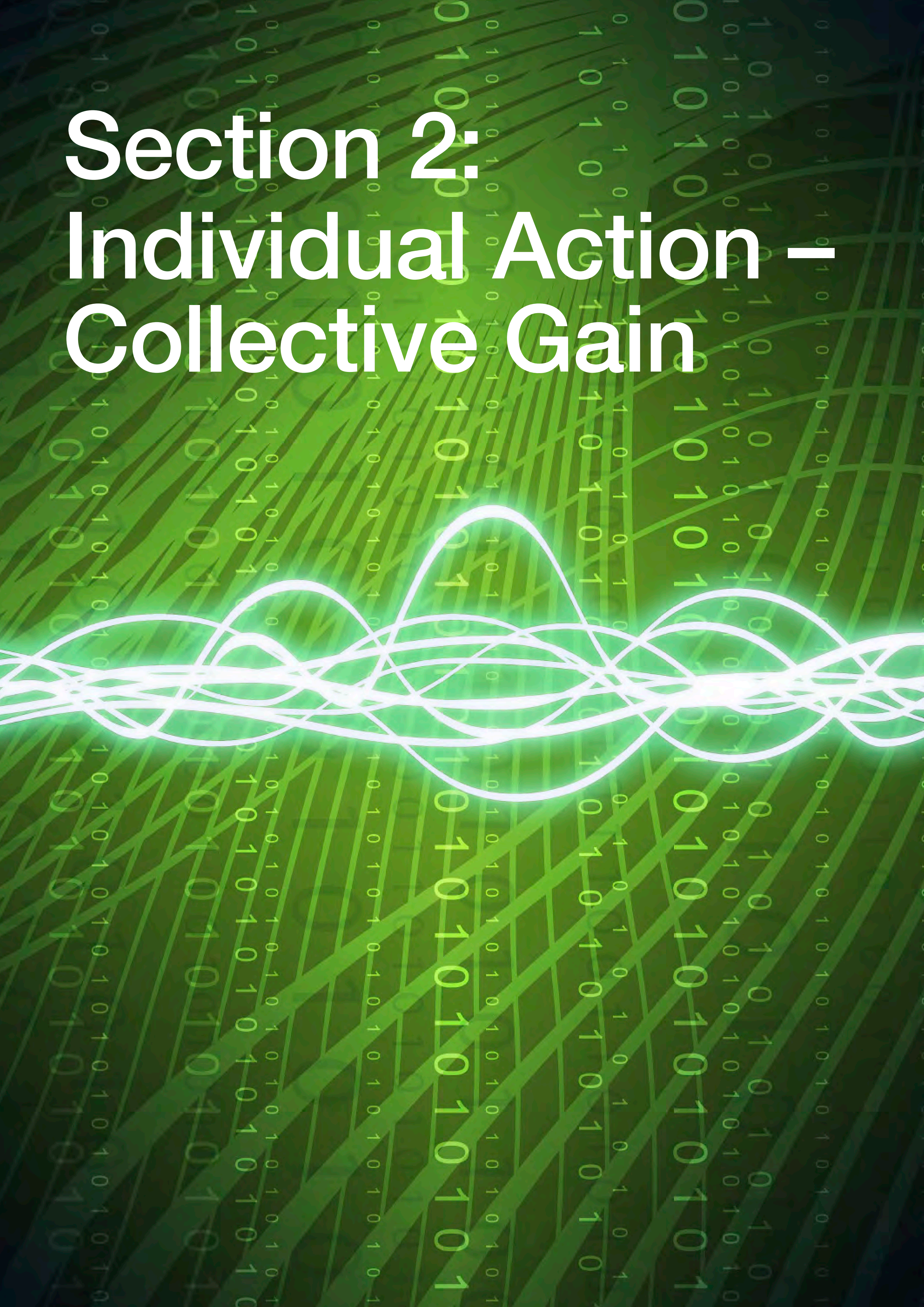
A number of responses to cyber threats have already been proposed among the international community. A first category of responses follows a traditional approach. This entails the adoption of policies and regulations to respond to the current cyber paradigm.

A second category of responses promotes a community-based approach. This entails, for instance, the sharing of information, mutual aid or coordinated action so that every stakeholder can mitigate cyber risk and contribute to a safer cyber environment. Several countries and international organizations are currently looking at the adoption of an international treaty that would apply in cyberspace.

A third category of response follows a systemic approach. This includes a new model for insuring organizations against breaches on their data held within the computing cloud, indicating the possibility that cyber risks could be quantified for the development of scalable risk transfer markets. Other examples are the use of technology to ensure "security by design" and thus create embedded security, as well as proposals to deploy a new Internet architecture that incorporates online identification.[12]

Nik Gowing, Main Presenter, BBC World News

Section 2: Individual Action – Collective Gain



Partnering for Cyber Resilience

The Partnership for Cyber Resilience initiative is a community-led initiative launched at the World Economic Forum Annual Meeting 2012 in Davos, Switzerland. Recognizing the interdependence of private and public sector organizations in today's global, hyperconnected environment, companies participating in the Forum initiative have an important role to play in contributing to a safer, more resilient digital environment. Together, this multistakeholder dialogue across numerous regions and sectors has led to the creation of the Partnering for Cyber Resilience Principles & Guidelines.

An organization's assets and reputation increasingly depend on secure and resilient cyber capabilities. An understanding of these risks and responsibilities is a critical component of the boardroom agenda.

By signing the Principles for Cyber Resilience, chief executives and their companies:

- Commit to the Principles, with an optional set of Guidelines providing a voluntary guide of best practice
- Individually demonstrate a company's commitment to best practice and corporate governance in a digital and connected world
- Collectively demonstrate private sector leadership in the ongoing policy debate on cyber issues
- Engage in dedicated private-public events that bring together signatories and policy-makers from different regions

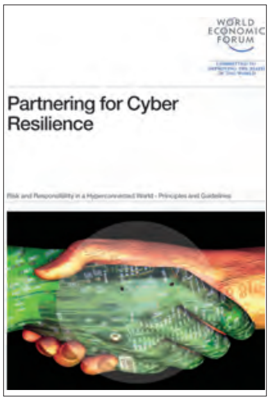
Cyber Resilience

Cyber attacks and incidents happen on a continuous basis. Given this reality, accepting that failures will inevitably occur at some point, leads to a more useful way of thinking about cyber security. In the event of a cyber incident, the objective should be to restore normal operations and ensure that an organization's assets and its reputation are protected.

The Partnering for Cyber Resilience initiative, therefore, defines "cyber resilience" as the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery. Cyber resilience is more than protecting computer systems with anti-virus software; it can only be achieved by adopting a holistic approach of the management of cyber risk. Stakeholders should integrate cyber risks management in their day-to-day operations and share information on threats and vulnerabilities among each other. While failures in the system are unavoidable, cyber resilience prevents networks and computer systems from completely collapsing.

Partnering for Cyber Resilience: Principles

- Recognition of interdependence: All parties have a role in fostering a resilient shared digital space
- Role of leadership: Encourage executive-level awareness and leadership of cyber risk management
- Integrated risk management: Develop a practical and effective implementation programme
- Promote uptake: Where appropriate, encourage suppliers and customers to develop a similar level of awareness and commitment


WORLD ECONOMIC FORUM
Partnering for Cyber Resilience
Risk and Responsibility in a Hyperconnected World - Principles and Guidelines

Guidelines for Cyber Resilience

The initiative contains a set of requirements that companies should aspire to meet at a minimum when implementing their own cyber risk management programme. According to the Guidelines, executive management teams are accountable for overseeing the development and implementation of an effective programme of best practices for cyber risk management within its broader risk management activities.

The Guidelines also recommend that the concepts and elements of the programme are integrated into the overall enterprise risk management programme where relevant. As any of the challenges result from unclear responsibilities of different organizations among the value chain, the Guidelines highlight the importance for companies to ensure that third parties and suppliers adhere to the programme and formalize this requirement using such contractual obligations. The Guidelines are non-prescriptive as specific standards, processes and legal requirements will vary by industry and jurisdiction and may change over time. While the Guidelines can be used to aid strategy development at the highest level, they are also consistent with and feeds into specific standards at the operational level.

Self-assessment Tool

The Partnering for Cyber Resilience initiative includes a tool for chief executives and other C-suite executives to help guide their internal review of their organization's cyber resilience capabilities. The tool is intended to provide executives with information to help inform their actions for the organization. It provides a rough composite score to locate the organization on a "hyperconnection readiness curve". The questions asked in the tool can also help executives to identify specific strengths and weaknesses – and paths to improvement within their respective organization.

Maturity Model

Drawing upon the results obtained through the self-assessment tool, the maturity model enables every company to locate itself in the "hyperconnection readiness curve". There are five different stages in the maturity curve.

Stage 1: Unaware	Stage 2: Fragmented	Stage 3: Top Down	Stage 4: Pervasive	Stage 5: Networked
The organization sees cyber risk as largely irrelevant. Cyber risk does not form part of the organization's risk management process. The organization is not aware of its level of interconnectedness.	The organization recognizes hyperconnectivity as a potential source of risk, and has limited insight in its cyber risk management practices. The organization has a siloed approach to cyber risk, with fragmented and incidental reporting.	The chief executive officer has set the tone for cyber risk management, has initiated a top-down, risk response programme, but does not view cyber risk management as a competitive advantage.	The organization's leadership takes full ownership of cyber risk management, has developed policies and frameworks and has defined responsibilities and reporting mechanisms. Leadership understands the organization's vulnerabilities, controls and interdependencies with third parties.	Organizations are highly connected to their peers and partners, sharing information and jointly mitigating cyber risk as part of their day to day operations. Staff show exceptional cyber awareness and the organization is an industry leader in managing cyber risk management.

Cyber Resilience as an Enabling Capability

In November 2011, the United Kingdom said that it wanted to become "one of the most secure places in the world to do business online". The idea that ICT contributes to growth and competitiveness through productivity gains is not new, but this statement shows an emerging discussion that security and trust in the online environment is by itself an important factor for economic gains.

> "There is a growing acknowledgement that cyberspace is the environment though which growth will happen. Not only are large amounts of money and time sunk into research but, whatever the time and money involved, knowledge is the fuel for innovation and entrepreneurship. This knowledge provides competitive advantage that is even more vital in developed economies where growth is otherwise up against a law of diminishing returns."[13]

This section highlights some exploratory links between ICT, cyber security, cyber resilience, institutions and competitiveness. To achieve these competitive gains, governments may have to develop new ways of working, both with the private sector and with other governments.

Information and Communication Technologies as a Driver of National Competitiveness

Information and communication technologies are indispensable and fully integrated aspects of competitive national economies. By enabling innovation and creating entirely new services and industries, the value of managed, structured, standardized networked information systems is greater than the sum of the parts that enabled it. The stability of markets and communities that results has a "compounding" effect, further enhancing the benefit.

The findings of the World Economic Forum's competitiveness reports have supported this idea, with a high correlation between a country's Networked Readiness Index and their competitiveness ranking observable over many years. Other studies have explored the consumer and business surplus accruing from the Internet, its productivity gains and other benefits.

Cyber Security and Economic Security

Protecting ICT infrastructure is a question of economic security. However, it also connects other assets, which are crucial to the functioning of the economy and society.

For example, the reliance of a country's economy and critical infrastructure on Supervisory Control and Data Acquisition (SCADA) networks[14] and computer systems has introduced vulnerabilities. The US Department of Homeland Security has identified 18 sectors as the nation's critical infrastructure and key resources, including water, agriculture, financial services, defence-industrial base, transportation systems and telecommunications.

The protection of national infrastructure is increasingly dependent on cyber resilience capabilities. A cyber attack against a system controlling power, water or transport, for instance, may have a serious impact on a country's security, public safety, health and economic stability. There is also concern that future attacks could cascade and cause greater effects, leading to severe social and economic disruption.

Financial flows – everything from high frequency trades to high street deposits – critically depend on densely connected and highly complex information systems. Liquidity is a function of trust, and with most of our money being held in denominations of 1s and 0s, a credible threat to the trust in the digital asset stocks and flows could result in a significant negative shock.

Cyber systems also enable supply chain optimization, lean processes and mass travel. As persons, objects and machines become more connected, disruptions could potentially have a high global impact across the global supply chain. A global drop in information flow will result in a global drop in trade and output. Ensuring resilient systems and infrastructure is therefore crucial to be able to manage, mitigate and respond to systemic risks emerging from the hyperconnected world.

Cyber Resilience for Competitive Advantage

The maintenance of a healthy cyberspace is not only a matter of national security, but it also increasingly defines competitive advantage in the global economy. In its Blueprint for a Secure Cyber Future,[15] the US government stresses that the increasing number and sophistication of cyber incidents has the potential to impact its economic competitiveness. Similarly, according to its cyber security strategy launched in November 2011, the United Kingdom took this a step further by saying that it wants to become the safest online environment in the world for companies to do business.[16] It has shifted the focus from treating cyber security as a defensive necessity to speaking about cyber resilience as a competitive advantage.

> "Increased reliance on and use of electronic data for real-time risk assessment, such as electronic manifests for cargo and advanced passenger information for air travel, have proven effective in facilitating movement of freight and people, but at the same time, puts more pressure on governments and businesses to maintain robust and secure information and communications networks that ensure a high degree of data integrity."
>
> – New Models for Addressing Supply Chain and Transport Risk, World Economic Forum

The idea that trust and security can be a source of value and competitive advantage for a business is not new. Credit and debit payment brands effectively monetize trust. Individuals and businesses will hesitate to engage in transactions with enterprises if they have concerns over the ability to secure their assets, be it cash, personal data or intellectual property. Statements like the ones from the United Kingdom above demonstrate that governments are starting to think about their attractiveness as a place to invest and locate operations in similar terms.

Just as in the case of companies, developing such a secure, trusted environment is not a function of technology alone. And just as public institutions provide the assurances required for markets to function elsewhere, many other non-technical factors will be the critical enablers of such trust. These factors are likely to include things such as clarity in the legal code, cyber forensic and investigative capabilities, professionals throughout the criminal justice chain who are capable of processing such cases, adherence to international standards, and formal and informal links with the private sector and across borders.

In recent years, governments have often talked about the shift to the knowledge economy, and recently some emerging nations have started to talk about strategies to speed up the "informatization" of their economies. In these contexts, policy-makers often focus on skills and education. However, it is only through a trusted and resilient network that information and communication technologies will be able to have an impact on growth and economic stability. This emerging dialogue suggests that developing such institutional capabilities may be another critical factor in achieving this goal.

Cyber Resilience Requires Collaboration

One of the factors required for a trusted digital environment highlighted above is the need for relationships with business and with other governments. Cyber security threats and responses demand new cooperation between the private and public sectors on a number of fronts, not least on the question of information sharing. Individual privacy, national security, innovation and economic activity must all be balanced, and this is only possible through trusted dialogue and collaboration between companies, the government and civil society. The Partnering for Cyber Resilience initiative, and the work the project is doing to identify common public capability requirements, can be seen as first steps in this process.

Cooperation is also required internationally, as the source and target of specific attacks are frequently not within the same jurisdiction. Domestic criminal justice agencies will need to be able to communicate with and rely on the assistance of counterparts abroad. Threat, response and best practice information may also need to be shared across borders. To this extent, no country can build a fully trusted, secure and resilient environment on its own.

From this perspective, competitiveness through cyber resilience is a relative objective rather than an absolute objective. A closed economy becomes brittle and open trade stimulates the domestic economy and enhances competitiveness. Likewise, countries which can coordinate to establish shared rules and common capabilities for a globally resilient cyber system will be best positioned to leverage the benefits for their own competitiveness.

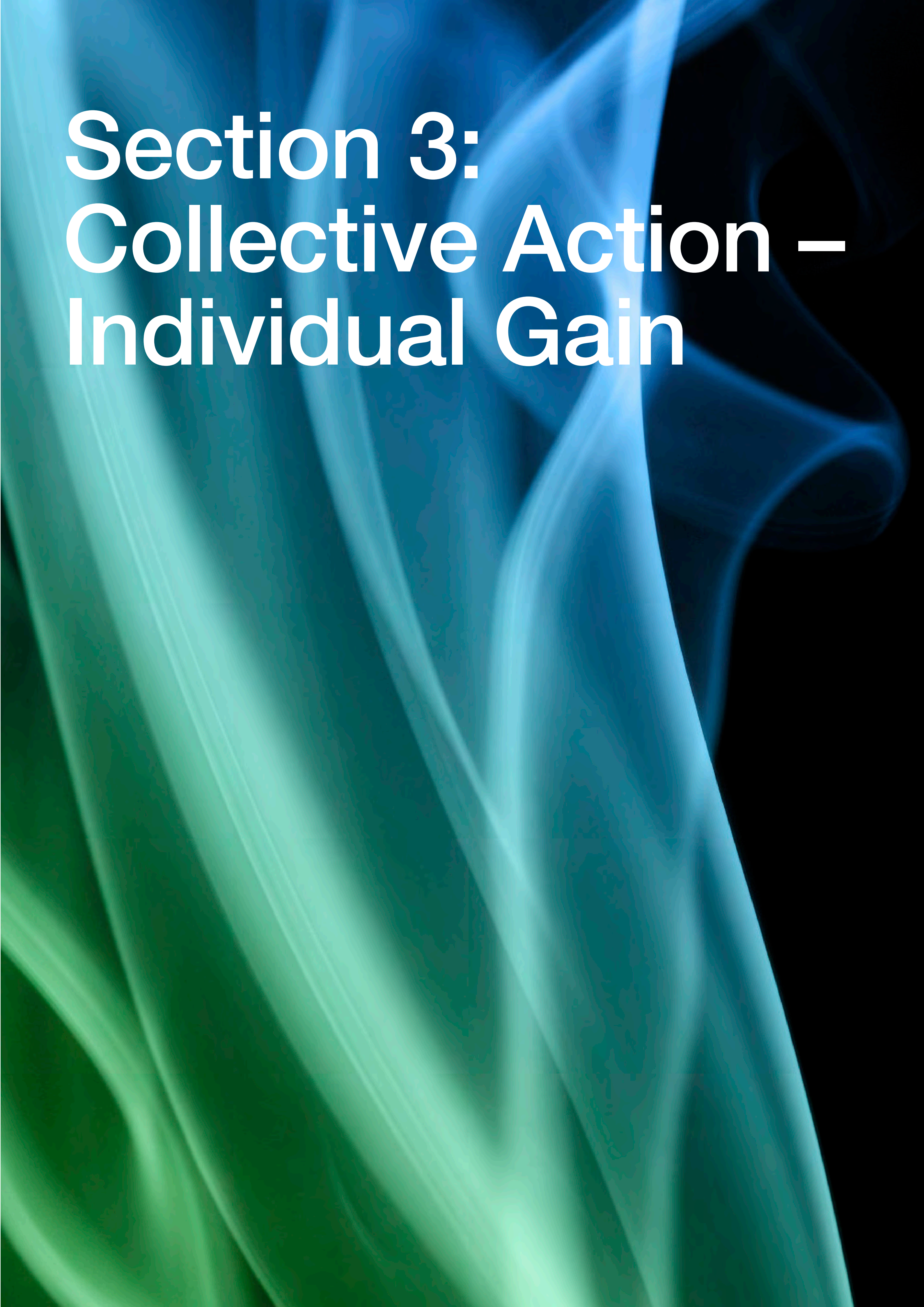
David Kirkpatrick, Founder and Chief Executive Officer, Techonomy Media; and Espen Barth Eide, Minister of Defence of Norway

While international treaties can be slow to put in place, raising questions for some about their effectiveness for dealing with cyber threats, governments can begin to harmonize and implement common capabilities which can help them communicate in common terms.

In some cases the link with trade is more than an analogy. For example, clear laws and credible criminal enforcement capabilities to prevent and respond to breaches of intellectual property rights are a relevant consideration in the attractiveness of an economy to potential corporate investment. Perceived weaknesses in this regard can not only be damaging to potential inward investment prospects, but can also be escalated to be a source of tension in international economic relations, with the potential for spillover into threats on other fronts of the trading relationship.

A second issue is the question of the interoperability of the Internet itself. It was highlighted above that a cyber attack on global supply chains could result in a drop in trade and output. It is worth noting that a fragmented online environment, whether due to multiple national firewalls or a fragmented policy environment, would have a more direct negative impact on trade and output, in particular in services. Such considerations emphasize the value for governments and companies to engage in a global dialogue to discover pathways to a globally resilient cyberspace that benefits all – “the tide that raises all boats.”

In questions of economic growth, the challenge is frequently one of finding the right balance between the markets that are the drivers of growth and the public institutions required to provide the conditions for sustainable and equitable markets. Markets are powerful tools to resolve complex coordination issues and optimize social gains; furthermore they operate globally. However, they do not always succeed in maximizing benefits and cannot operate in isolation. As such, the next section highlights some of the emerging thinking on the economics of cyber security.



Section 3: Collective Action – Individual Gain

Economics of Cyber Security

Market forces are often an efficient and effective way to solve issues. However, for several reasons they are not adequately responding to some of the aspects of the hyperconnected world. These reasons include externalities, information asymmetry, and the challenges in understanding the value of security. Potential solutions to help the market respond to cyber risk include the reinforcement of incentives, the creation of an increased accountability, the strengthening of the impact of liability through penalties or disclosure rules, and the use of cyber risk insurance as a way to limit liability and encourage risk reduction.

Challenges

Security Value

From a board's perspective, investing in cyber security is usually not high on the agenda of stockholder meetings. The investment may be significant, and unless the company has a way to market its security capabilities there is no immediate upside to the investment. The true value of cyber security, then, is hidden in the effect this "unrewarded risk"[17] may have on an organization.

Traditional cost-benefit analysis will suggest that an organization seeks to maximize profit by minimizing cost. Thus, the optimal investment in security is determined by the perceived relevant threat to the organization, the related risk to its assets and reputation, and the monetary loss associated with the risk occurring, expressed in the value of missed opportunities, interrupted operations, stock value loss or otherwise. It is the method many organizations try to use, with varying degrees of success, to quantify security decisions.[18]

Following this reasoning, the value of security measures equals the decrease of potential loss caused by the cyber risk when it occurs. This equation would have a near infinite number of variables and thus require a series of assumptions to solve within a reasonable margin of error. Additionally, while the odds of suffering a serious breach may not be perceived to be very high, the associated impact with that breach may be beyond the organization's risk appetite.

> "Today there are no real consequences for having bad security or having low-quality software of any kind. Even worse, the marketplace often rewards low quality. More precisely, it rewards additional features and timely release dates, even if they come at the expense of quality."
>
> – Bruce Schneier, Security Technologist and Author

Externalities

The lack of definition and understanding of cyber risks represent one of the main challenges in dealing with cyber risk. Quantifying the harms of an attack, the motives of many different types of adversaries and determining the likelihood of an incident has proven quite difficult. Lacking these basic tools of risk analysis, decision-makers may be tempted to focus on that which they can address – leaving vulnerabilities undealt with.

The value of security spending is hard for organizations to quantify and justify. Determining the marginal value of another layer of security in a multi-layer strategy is challenging for an organization. Trends towards massive inter-organizational dependencies further amplify the problem. As organizations interact with one another, it may be difficult for them to understand and measure what risks are upstream and downstream from them and the value of security to and from business partners and customers. The boundaries of risks and responsibilities are being reset in the hyperconnected world.

This "networked world" externality also drives the uptake, or lack thereof, of security protocols or technology. For some technology, such as DNSSEC,[19] the benefits will only emerge when a critical mass has adopted the technology. There is limited first mover advantage and no immediate positive return on investment (ROI), so the willingness to adopt this technology is low. Additionally, due to increasing hyperconnectivity, "free riding" may become an issue: the actions of others may benefit you, reducing the need for you as an individual to take action – if others take care of some of the issues, the motivation to act goes down. Some may choose not to invest, either because they feel they would be taking care of a shared problem, or because they feel their investment does not yield its full potential unless everyone does the same.[20] Similarly, the "tragedy of the commons" applies to cyberspace as well – key actors may take actions that benefit all but them, which make for a bad business case in most companies. These factors limit motivation to deal with the issue.

Tetsuo Yamakawa, Vice-Minister for Policy Coordination, Ministry of Internal Affairs and Communications, Japan; Ray Lane, Executive Chairman of the Board of Directors, Hewlett-Packard Company; and Neelie Kroes, Vice-President and Commissioner for the Digital Agenda, European Commission

Information Asymmetries

While the potential upside to security (i.e. a positive return on investment from having better security in organizations or in the development of specific products seems intuitive, the reality is that this effect may not consistently apply. Market actors do not always have information regarding the relative security of potential business partners in order to use security as a factor in decision-making. Even if a product is technical in nature and where security is a component, customers lack information to discern whether the security component is better, or even a differentiator. The market would need better information in order to make that determination. This drives vendor behaviour – vendors may assert their software is secure, but buyers cannot tell, and refuse to pay a premium for quality, so vendors invest in marketing rather than engineering.[21]

As detailed in this report's Information Sharing chapter, there are many reasons for actors to refrain from sharing information to combat threats or breaches. Regarding security capabilities of products and services there is, perhaps, even less incentive to share information. In the case of applications, for example, frequent "patching" to resolve security issues may be positive and responsible behaviour, but it may also signal a poorly designed product to users. Even the release of a patch to fix a security issue poses a risk in and of itself, as hackers will reverse engineer the patch provided by the supplier, and then use this information to target attacks to unpatched systems. Information asymmetry is especially tangible in the event of "responsible disclosure," where there may be a significant duration between the discovery of a security issue and the release of a patch. This grace period is intended to allow for the development of the patch, but once the flaw has been discovered by others than the original developers (either through leaking by someone involved or by the publication of the patch), exploits and attacks may occur.[22]

The difficulty in defining the value of security, in sharing of information and in dealing with microeconomic behaviour does not need to result in comfortable inaction however, but rather it can be dealt with using principle-based solutions.

Potential Solutions

Reinforcement of Incentives

A primary way to substantiate the need for cyber security investments is to revise and reinforce incentives. Security failure is caused by bad incentives at least as often as by bad design.[23] It is useful to consider how incentives can be introduced or amplified to help market mechanisms respond to the economics of security. The challenge is then to transform security spend from a shareholder cost to a competitive advantage.

The first step towards revising incentives is to ensure that information security decisions are seen more broadly than the traditional narrow domain of the chief information officer – it affects the entire organization and is thus a matter of corporate governance, requiring the attention of the board and the chief executive officer. Secondly, a top-down effort to instill a sense of "cyber hygiene" into the organization is required to ensure that the mindset shifts towards a sense of cyber responsibility. At the products and services level, organizations can leverage their own purchasing power: as they create specifications for development of software and hardware, it is a relatively easy step to include security requirements. Providers would then need to comply and incorporate the security features to stay competitive.

Increased Accountability

The need for accountability is not unique to cyber security, but there are some unique features. One approach to introducing accountability is the voluntary adoption of standards and norms. While quality standards and industrial norms have been around for a long time, specific norms related to cyber security have been developed in conjunction with the advance of (and reliance on) information technology. A great variety of rule-, objective- and principle-based cyber standards now exist. To be useful, standards must be flexible enough to allow for the rich diversity across covered entities and nimble enough to require only that which is necessary, all while still wielding enough power to drive the needed change and provide a signalling function to other actors.

Voluntarily accepting norms and standards is a strong quality-signalling function, similar to a voluntary audit on financial statements for private companies. Proactively complying with norms, joining industry partnerships or incorporating a transparent risk management approach can be used as a competitive differentiator.

Another approach is for governments to intervene. Current cyber legislation is a patchwork, making it a challenge for organizations, particularly those that participate in online markets, to understand and comply with the varying local requirements of different jurisdictions. This has led many to call for an international accord or harmonization of laws governing cyberspace.[24] Regulation, however, may not be preferable for some organizations or industries due to scale or regional complications. Additionally, due to the rapid developments in technology, a principle or process-based approach would increase effectiveness and longevity of any potential regulation.

Cyber regulation already exists, but to a lesser extent than, for instance, privacy regulation. There has been a significant increase in interest in 2011 and 2012 into cyber regulation, illustrated by the debate on the Cyber Intelligence Sharing and Protection Act (CISPA),[25] a proposed US act which would enable extensive information sharing between corporations and the US government to counter cyber threats. CISPA does not require organizations to implement specific tools or risk mitigation measures, unlike the Gramm–Leach–Bliley Act, which requires financial institutions to protect against any anticipated threats or hazards to the security or integrity of customer records.[26]

Liability

Much of the discussion on liability focuses on what penalties governments can impose. Penalties may result from incidents or from non-compliance with a regulation or standard. Data breach disclosure requirements thus offer a disincentive based on negative impacts to immediate financial performance, stock price and reputation. As organizations determine who will assume the liability of the hyperconnected relationship they share, any unexpected or catastrophic financial or legal event has the potential to disrupt innovation and growth.

Natarajan Chandrasekaran, Chief Executive Officer and Managing Director, Tata Consultancy Services

Liability avoidance in the traditional sense within the present cyber security market is put in place contractually between business partners and customers. These contractual agreements can even be one-sided, such as software license agreements shown during the installation of software, for instance. These agreements absolve the software developer of liability.

Insurance and Reinsurance

Virtually every established industry in the world relies on risk transfer insurance models to address liability. The hyperconnected world also has the potential to seek systemic stability by employing a risk-transfer structure, taking asset and reputational risk away from its participants and to a third party.

The cyber risk insurance market is approximately US $ 800 million in premiums, increasing in volume by roughly 30% in each of the past two years.[27] With reinsurance products not readily available yet, the current market shows the characteristics consistent with that of an emerging market as insurance providers enter and exit as the market evolves.

Early adopters of cyber insurance are typically from high-risk industries, for example organizations that hold large amounts of regulated data, such as those in the financial services, healthcare and retail industries. This type of adverse selection by customers, where only those who really need the insurance purchase it, can lead to growing pains in a nascent market. As was the case in the long-term care insurance market, the risk was not well understood by insurers who entered that market early but have since reconsidered.[28]

Should insurers learn from that example versus following the same path, one would expect limited scope of coverage and higher prices to prevail. Organizations with a lower technology risk profile may choose to self-insure instead, if a market-clearing price cannot be established. Future government actions related to accountability has the ability to significantly impact the risk landscape going forward.

Information Sharing

Private-public partnerships are crucial to mitigate cyber risks and foster collaboration to improve cyber resilience. Among them are information-sharing initiatives, which help governments and businesses prevent, protect, deter and recover from cyber threats. While partnerships have been established, several challenges still prevent stakeholders from reaping the full benefits of information sharing. The need to build trust among parties and share actionable information is crucial. Jurisdictional boundaries, the fear of being held liable, and the quality and quantity of information shared still represent major barriers to information sharing.

Information sharing refers to the exchange of a variety of network and information security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice.[29] While this definition seems straightforward, one of the main issues related to information sharing is the lack of consensus on its various components. A common dialogue on the framework required to share information is needed to identify existing gaps and find appropriate solutions.

While some initiatives are already in place, organizations are still reluctant to exchange sensitive information with others. In fact, the existing challenges and barriers often outweigh the incentives in sharing data with other organizations.[30] This section seeks to create a clear and consistent taxonomy of these issues, as well as address key questions related to information sharing. What are the challenges and barriers to information sharing? Why are organizations reluctant to share information? What level of trust is required? What kind of dialogue is needed and can key trade-offs be identified?

Actors

Public Sector

As governments have become more reliant on interconnected computer systems to support critical operations, the need has increased to have a strong process to identify the most critical systems in a nation and to ensure their protection. Several countries have already created sector-specific information-sharing partnerships between the government and the private sector, such as the Information Sharing and Analysis Centres (ISACs), the United Kingdom's Centre for the Protection of National Infrastructure (CPNI), Australia's Trusted Information Sharing Network (TISN) for critical infrastructure resilience and the Spain's Grupo Trabalho Securidad (GTS).

Government can serve as a convener to bring different parties together as well as facilitate and coordinate actions among stakeholders. When government serves in that role, it is critical that it is willing – and legally able – to share information that is as sensitive and actionable as what it expects to receive from private sector participants. If the flow of information is one way, then the value proposition of the exchange can be diminished. In addition, the government can act as a "safe harbour" for companies to share data and address some of the existing challenges related to information sharing, such as the fear of anti-trust action or legal liability for the information.[31]

Private Sector

Sharing information can be helpful for companies attempting to gauge whether they are accepting similar or generally acceptable levels of risk compared with their peers. While the private sector owns the majority of the infrastructure and is directly impacted by a cyber incident, some companies may lack incentives to share information and collaborate with others.[32] There is, thus, a strong need to raise awareness within each company, both in the boardroom and at an operational level.[33] Several information-sharing initiatives are already in place. Intra- and inter-ISAC information sharing can and does occur. And, there is at least one example of a cyber incident response organization being established that is entirely separate from the public sector – the Industry Consortium for the Advancement of Security on the Internet (ICASI) – which looks at multi-product security challenges that may impact the Internet.[34]

Public-Private Partnerships

Two types of approaches among the existing initiatives can be observed. The first approach is a vertical or a sectorial one and aims to divide information sharing by sectors. The second approach seeks to compile various sectors together and create a cross-industry dialogue and response. To be valuable, information (particularly actionable information) needs to be shared among governments and companies. Public-private partnerships in information sharing enable organizations to avoid the duplication of effort and fill potential gaps in information security capabilities. It also leads both the governments and the industry to define their own role and responsibilities to reduce cyber risks and find a shared approach to deter, protect, prevent, respond and recover from cyber attacks.

Levels of Communication

Strategic

In line with its fiduciary and other leadership duties, the executive leadership also has a crucial role to play in the field of information sharing. The executive leadership could create a culture of information sharing about critical dependencies and risks that exist inside an organization, and create an environment to address critical risks quickly. The exchange of cyber security risk information among organizations enable companies and governments to develop a full plan to improve cyber resilience based on best practices and lessons learned from others, or to partner in the creation of a broader national plan as was the case with the US National Infrastructure Protection Plan. Furthermore, the executive management team is in the best position to set an overall programme for information sharing, as well as provide support and resources to implement it at each level of the organization.

Operational

Robust information sharing and coordination must also happen at an operational level. To be effective, information must be shared not only by the executive leadership team, but also by managers with day-to-day operational responsibility. The exchange of data needs to be integrated into the organization's on-going risk management practices and policies. Operationally, the organization should also have routine points of contact with major partners, vendors, suppliers and customers to exchange information and receive reports about incidents or issues, preferably through a centre of excellence for operational risk and security issues.

Technical

In the event of a cyber incident, information sharing tends to increase, as a larger number of companies and government entities have a vested interest in sharing more information to meet a common goal. Once the incident has concluded, entities return to their more normal state of sharing a limited or tailored set of data. It is critical that companies have clear and trusted points of contact with whatever information sharing clearinghouse it may use (Information Sharing and Analysis Centers, Computer Emergency Response Teams, a national incident management capability, a local law enforcement agency, etc.) so that when a cyber incident begins, the organization can draw on known contacts and familiar processes until a normal operational state is achieved.

Information Type

Threats

In today's risk environment, public and private organizations are exposed to sophisticated and complex attacks. An organization needs a clear understanding of the threats against its own network and systems, as well as its interdependencies with major threats to external organizations and ICT infrastructures. Having a strong internal culture of threat modelling, managing alerts, risk assessment and mitigation will go a long way towards understanding the threat environment. Organizations can also benefit from data gathered by external sources to help create a broader view of the cyber risks that they are facing.[35] Having information on threats and actual incidents experienced by others can help an organization better understand the risks it might face and decide upon their response. While some organizations already have access to relevant data, they may not have the tools and analytic capabilities to make use of these data.

The exchange of comprehensive and timely alerts and information on attacks can help private and public organizations determine the nature of an attack, implement a mitigation strategy or advise others on how to respond to an imminent attack. It enables an organization to gather the most up-to-date threat data, integrate it in their systems and processes, make real-time decisions and take defensive action.[36] As such, an organization is able to seek help from other organizations to take appropriate measures to ward off an imminent attack and build a coordinated response.

Vulnerabilities

Perpetrators of cyber attacks are keen to exploit vulnerabilities for which there is no known fix. These "zero-day" vulnerabilities are important pieces of information. Information sharing on zero-day exploits should be done with care to prevent further harm. Sharing information about vulnerabilities and new discovery helps organizations address weaknesses before they are exploited and shift from reactive to proactive security measures. Sharing information on known and "fixable" issues can also be important, as a matter of good corporate citizenship.

Information-sharing Lifecycle

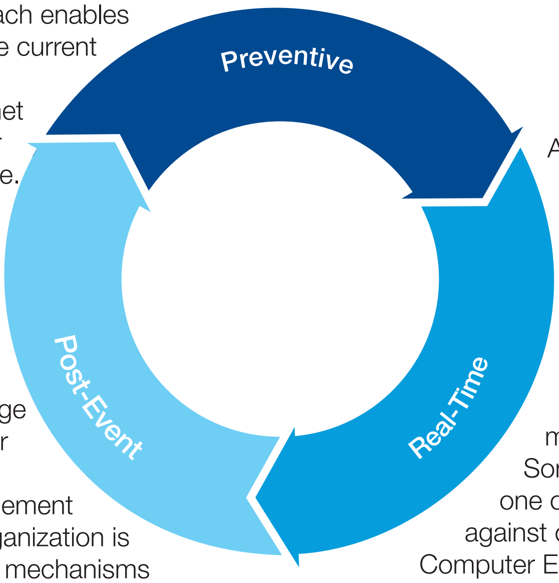
The exchange of information may happen at different stages of the security lifecycle. In practice, a majority of information sharing is preventive, (i.e. applies to threats that could happen in the coming six or nine months) or in real time (i.e. applies to incidents that are about to happen or have just happened).

> "Trust and value grow together but need investment. If trust is broken it is slow and difficult to rebuild. With maturity of trust comes greater value as the higher the trust, the more people feel able to share."
>
> – Good Practice Guide, European Network and Information Security Agency (ENISA)

Relevance of Trust

Trust is a key prerequisite for information sharing; a lack of trust may prevent organizations from sharing information with one another. IT professionals in organizations are often fully aware of risks in their organizations' infrastructure. They will also be able to determine whether information available to them is actionable and relevant. To develop trusted relationships, every party has to be willing to contribute information of value to ensure that the parties stay engaged and work towards a common approach to problem-solving.[37] False negatives and false positives are detrimental to parties' incentive to share information.

Because of the speed and pervasiveness of cyber threats, a preventive strategy is needed. A preventive approach enables an organization to assess the current threats and define a set of capabilities that should be met when implementing its cyber risk management programme.



A real-time response occurs while a cyber incident is ongoing and may, for example, facilitate emergency preparedness, request for help or warning to others. To ensure such a response, an organization needs to establish a systematic approach to manage alerts, oversee the network attacks and monitor responses to incidents. Some organizations are already using one or more real-time sources to react against cyber attacks. Examples are the Computer Emergency Response Agencies (CERT), which provide reports or advisories on threats and vulnerabilities as well as attack indicators.

Information sharing may also relate to a cyber incident that is no longer active. It enables an organization to take advantage of lessons learned from other organizations and integrate these in its cyber risk management programme. As such, an organization is able to improve its response mechanisms and prevent future threats and attacks.

Since information sharing often implies the disclosure of weaknesses, vulnerabilities or other sensitive information, parties need to trust the environment in which they share information. Participants may fear that sharing certain information could affect their reputation, damage customer trust or could be used by a competitor.[38] This is also the case for government representatives who may be concerned about leaks of classified information.

To improve information sharing dynamic, requiring each participant to contribute and share information may prevent "free-riding." Similarly, it may prevent a tendency to underinvesting in security measures as the exchange of information can be used as a partial substitute.[39] Furthermore, ensuring consistent participation by parties helps build relationships among participants.[40]

Finding a balance between openness, transparency and inclusiveness may be a long process and require significant effort, but it is a crucial step to successful information sharing. Once members of the group trust the environment and the information they obtain, the increased attractiveness of the information sharing network may promote its use and growth.

Challenges and Barriers

Jurisdictional Boundaries

While cyber attacks may effortlessly cross geographic borders and jurisdictional limits, information sharing in an international setting is not as easy due to legal and cultural differences. Difficult as it may be, international information sharing is crucial to deter and mitigate cyber threats.

Several international initiatives have already been established to enable information sharing between governments and companies from different countries. The European and Network Information Security Agency (ENISA), for example, has actively promoted information sharing. ENISA developed a Good Practice Guide on Information Sharing[41] in 2009, which aims to assist member states and other relevant stakeholders in creating and running network security information exchanges. Similarly, the International Multilateral Partnership Against Cyber Threats (IMPACT), the operational arm for cyber security of the International Telecommunication Union (ITU), is an international public-private initiative seeking to improve the global community's capacity to prevent, defend and respond to cyber threats.[42]

Liability

The purpose of an adequate environment for information sharing is to exchange real-time and relevant information that organizations can use to take measures to deter cyber threats, respond to cyber attack and maintain cyber awareness.[43] The more timely and practical the exchange of information, the better chance stakeholders have to keep pace with cyber attacks and reduce cyber risks.[44] In the current environment, some organizations may still be hesitant to share information with others, as they fear to be held liable for the information they are disclosing. Liability concerns are a major barrier for information sharing and may be divided into two categories. First, entities may be reluctant to share information as they are concerned that the information they are disclosing would be lost or used for other purposes than the ones to which they agreed. Second, organizations from the private sector may fear that the information they are exchanging with the government would be used as the basis for determining a violation of civil or criminal law.[45] Clarity on the extent of parties' liability or possibly "hold-harmless" policies may be required to deal with the liability concerns.

Accountability

While countries seek to secure their digital network against cyber attacks by promoting better online transparency and accountability, human rights advocates emphasize the importance of online anonymity to promote free political discourse.[46] Many governments are facing two potentially conflicting interests. The first is to prevent their infrastructure and networks from cyber attacks. The second is to promote human rights by enabling online communication of ideas. Finding a balance between the right to privacy, freedom of expression and the mitigation of cyber risks poses a significant challenge. In addition, organizations may not necessarily act as a coherent body and can be driven by different internal motivations and objectives. The decision to be part of an information-sharing group may be, for this reason, difficult to make as the possibility to disclose information may vary within an organization.

Public Sector and Private Sector Imbalance

Some private sector entities are reluctant to share information with the government as they may feel that there is an imbalance between the information they disclose and the information they obtain in return. The Information Technology Industry Council observes that the information shared by the government is often too generic or outdated to be useful.[47] Furthermore, information shared by the public sector is often classified and can only be shared with those with security clearance.[48] The government may also be hesitant to share information with membership-driven groups as they feel that disclosing such information would be “unfair” to non-members. Private sector companies may even feel that sharing information with the government is by itself a security risk as government organizations are prime targets of cyber attacks and by no means immune.[49]

Limits to Information Sharing

Important progress has been made in using and promoting information-sharing organizations. However, some challenges still limit the information flow between the public and private sectors. While many organizations recognize the importance of information sharing, some observe that there are still gaps on the “how, what, when and to whom.”[50] Several factors, such as challenges related to the management and organization of the group, the risk of reputational damage, legal repercussions and the lack of clear agreements and expectations, may explain why the current environments are not fully effective.[51]

Case Studies

The tables below seeks to provide an overview of the functioning, challenges and incentives of two existing information sharing initiatives – one national from the US-based Information Technology Information Sharing and Analysis Center (IT-ISAC), and one international from the European Public Private Partnership for Resilience.

Information Technology Information Sharing and Analysis Center (IT-ISAC)

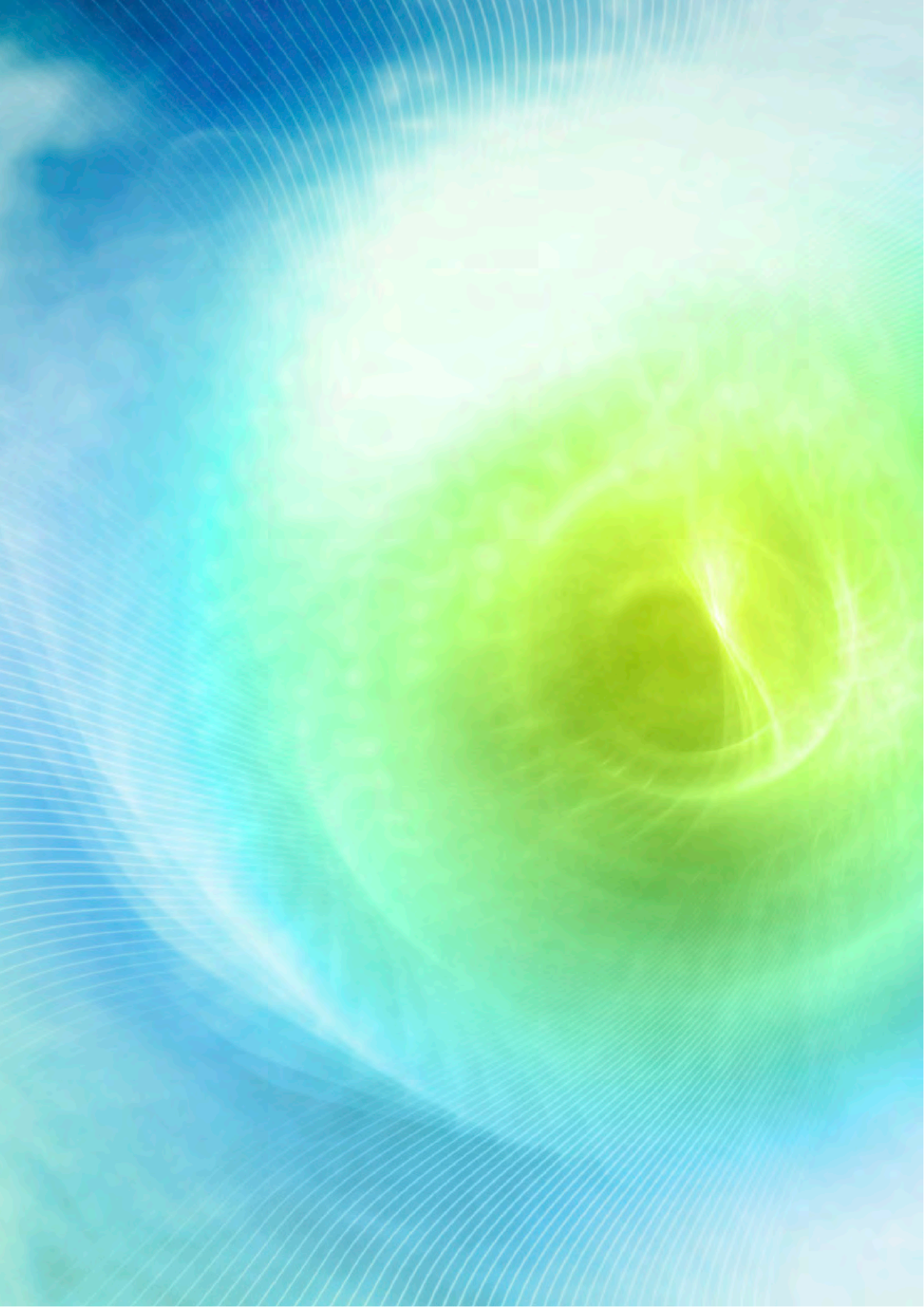
Actors	■ Consists of 24 members, mostly IT companies, who are vetted as members and utilize secure communications channels for sensitive information sharing ■ Seeks to partner and liase with the US government and routinely exchange actionable and meaningful threat and vulnerability information with the public sector[52] ■ Drives informed decision-making by policy-makers and industry as a trusted sector-wide advisor on IT sector security response and cyber information sharing issues
Levels of Communication	■ Operational services such as risk mitigation, incident response and information sharing that protects the nation’s critical infrastructure ■ Interactions between cyber security specialists, enabling peers from other member companies to share and understand non-public details of threats and vulnerabilities. ■ Technical support to analyse and address cyber threats
Information Type	■ Security incidents ■ Threats ■ Attacks ■ Vulnerabilities ■ Solutions and countermeasures ■ Best security practices and other protective measures[53]
Information-sharing Lifecycle	■ Shift focus from vulnerabilities to threats and indicators as it realized its members needed more timely, high-quality, analysed information on threats to preventively mitigate risks to their companies and customers[54] ■ Provides members with a trusted point of contact for information sharing prior to and during incidents ■ Disaster response
Trust Aspects	■ Membership is vetted and requires contractual agreement specifying information requirements and specified levels of confidentiality. Certain information is limited to only IT-ISAC members; formal information sharing protocols include a confidential forum in which threat and other data are shared anonymously ■ Certain alerts and analytical information are also shared beyond the membership to trusted organizations using specified protocols ■ Development of internal communities focused on specific issues of common interest[55] ■ Three membership levels (Participant Bronze, Premium Silver and Foundation Gold)[56]

Incentives	■ Provide comprehensive sector analysis and have the ability to reach extensively within their sectors, with other sectors and with government to share critical information ■ Security and “all hazards” response: critical technical, IT/cyber and physical infrastructures and cross-sector interdependencies are analysed and addressed ■ Provide operational services such as risk mitigation, incident response and information sharing that protects the nation’s critical infrastructures ■ Forum for experts within member companies to engage in trusted information exchange, analysis and communications related to all aspects of cybersecurity risk management ■ Empower business resiliency through security planning, disaster response and execution (most ISACs, by definition, have 24/7 threat warning, incident reporting capabilities which are critical to the success of protecting critical infrastructure)
Challenges	■ Maintaining the funding commitment to support an independent operations centre and necessary security management controls, staff a 24/7 capable operational capability, and support administrative and management functions ■ Committing internal company expert participation and integrating the IT-ISAC operational construct into a member company’s operations ■ Growing the membership requires clarifying of cross-industry relevance and importance of the ICT sector as an infrastructure provider ■ Establishing more robust trusted communications with governments and gaining regular access to actionable threat information available only from government sources

Philip Harrington, Executive Vice-President, Risk, and Chief Administrative Officer, CA Technologies; and Jolyon Barker, Managing Director, Global Technology, Media & Telecommunications, Deloitte Touche Tohmatsu Limited

European Public-Private Partnership for Resilience

Actors	■ Experts from Telecom sector: operators, manufacturers, regulators, member states ministries ■ The European Commission is represented by experts from the Directorate-General INFSO (Information Society, soon to be renamed DG CONNECT) and ENISA
Levels of Communication	■ Strategic management ■ Tactical
Information Type	■ The EP3R knowledge base constitutes issues challenges, barriers met by industry to the improvement of security and resilience measures, keeping cross-border and competition dimensions as a prime requisite
Information-sharing Lifecycle	■ Three groups are focused on preventive action ■ One umbrella group is focused on botnets
Trust Aspects	■ Trust among participants is gradually built ■ Creation of a solid membership and build a good administration of the group ■ Establishment of clear rules within the group ■ Encourage members to participate in the discussion as experts and privilege the interests of the group over their own interests ■ Alignment of incentives; as there are continuously newcomers, crucial to adjust the value proposition and make sure that incentives are well understood
Incentives	■ Provide regulator(s) with the industry's point of view on important issues, thus allowing the elaboration of more efficient and effective rules and regulations (and avoid regulation when inappropriate)
Challenges	■ Maintain present engagement and proper resources ■ Gain commitment from the industry as it is still difficult to obtain engagement and implementation from the private sector



Conclusion

This document has highlighted some of the key outputs and emerging issues related to cyber resilience that have been raised over the first year of the Risk and Responsibility in a Hyperconnected World project.

While there has been much dialogue on the topic of cyber risk, one gap highlighted by the Partnership for Cyber Resilience initiative has been the need to focus on corporate governance and to raise the profile of cyber risk with corporate boards and chief executives, so that it receives greater focus and is included in ongoing decision-making.

Providing executives with information and tools to understand and mitigate the vulnerabilities within their organizations presented itself as one way to create immediate impact. This led to the development and launch of the Partnering for Cyber Resilience initiative, a set of principles to promote cyber resilience. By signing the Principles, chief executives and their companies commit to improving cyber resilience. They are also provided with an optional set of guidelines that serve as a voluntary guide of best practice. Signatories individually demonstrate their commitment to best practice of corporate governance in a digital, connected world and collectively demonstrate private sector leadership in the ongoing policy debate on cyber issues.

In particular, the Principles focus on:

- Recognition of interdependence: All parties have a role in fostering a resilient shared digital space
- Role of leadership: Encourage executive-level awareness and leadership of cyber risk management
- Integrated risk management: Develop a practical and effective implementation programme
- Promote uptake: Where appropriate, encourage suppliers and customers to develop a similar level of awareness and commitment

Throughout the initiative, the concepts of resilience, governance, trust and complexity underlined the challenges and solutions needed to address challenges of the hyperconnected world. In addition, the dialogue surfaced some concepts that require more public debate before being addressed:

Cyber resilience as an enabling capability – Access and usage of Information and Communication Technologies (ICT) encourage the growth of work forces, and increase productivity gains, as well as improve its public services and, thus, increasing the level of trust of citizens. Cyber resilience is, as such, considered a key factor in determining a nation's competitiveness in today's global economy; economic security strengthens social cohesion and political stability. The governments of the United States, the United Kingdom and other nations have emphasized the need to build national capacity through public-private partnerships to focus on creativity, innovation and entrepreneurship and enable cyber competitiveness. While there appears to be an intuitive consensus among governments and businesses that cyber resilience is a critical enabler of growth and stability, some challenges and differences in capabilities still prevent them from fully harnessing the benefits of the hyperconnected world.

Economics of cyber security – Market forces are often an efficient and effective way to solve issues. However, for many reasons they are not currently working to solve the problems associated with hyperconnectivity. These reasons include externalities, lack of information on the quality of security for products and services to incorporate in buying decisions, and the challenges in understanding the value of security. Concepts for changing this include:

- Strengthening incentives such as encouraging sharing of security information as a differentiator, potentially in the form of ratings, and the use of government buying power to drive security into product specifications
- Increasing accountability by the voluntary adoption of standards and norms
- Encouraging government and boards to hold organizations accountable
- Intensifying the impact of liability through penalties or disclosure rules
- Exploring the use of cyber risk insurance as a way to limit liability and through pricing, encourage risk reduction

Information sharing – Both the private sector and governments recognize the benefits of information sharing and the need to leverage resources and information and collaborate across sectors to prevent, protect, deter and respond to cyber threats. While there is a strong consensus that public-private partnerships are crucial to the success of information sharing, some barriers still affect the sharing of information between governments and companies. The creation of trust among participants represents one of the main challenges; the participation of regulators and the fear to be held liable are also a significant barrier to information sharing. In addition to the importance of building a trusted environment, many recognize the need to improve the ability to act on what is shared, and help governments and enterprises know what to do when a cyber threat occurs. Actionable information is critical to add value for participants and to ensure that sharing will occur over time.

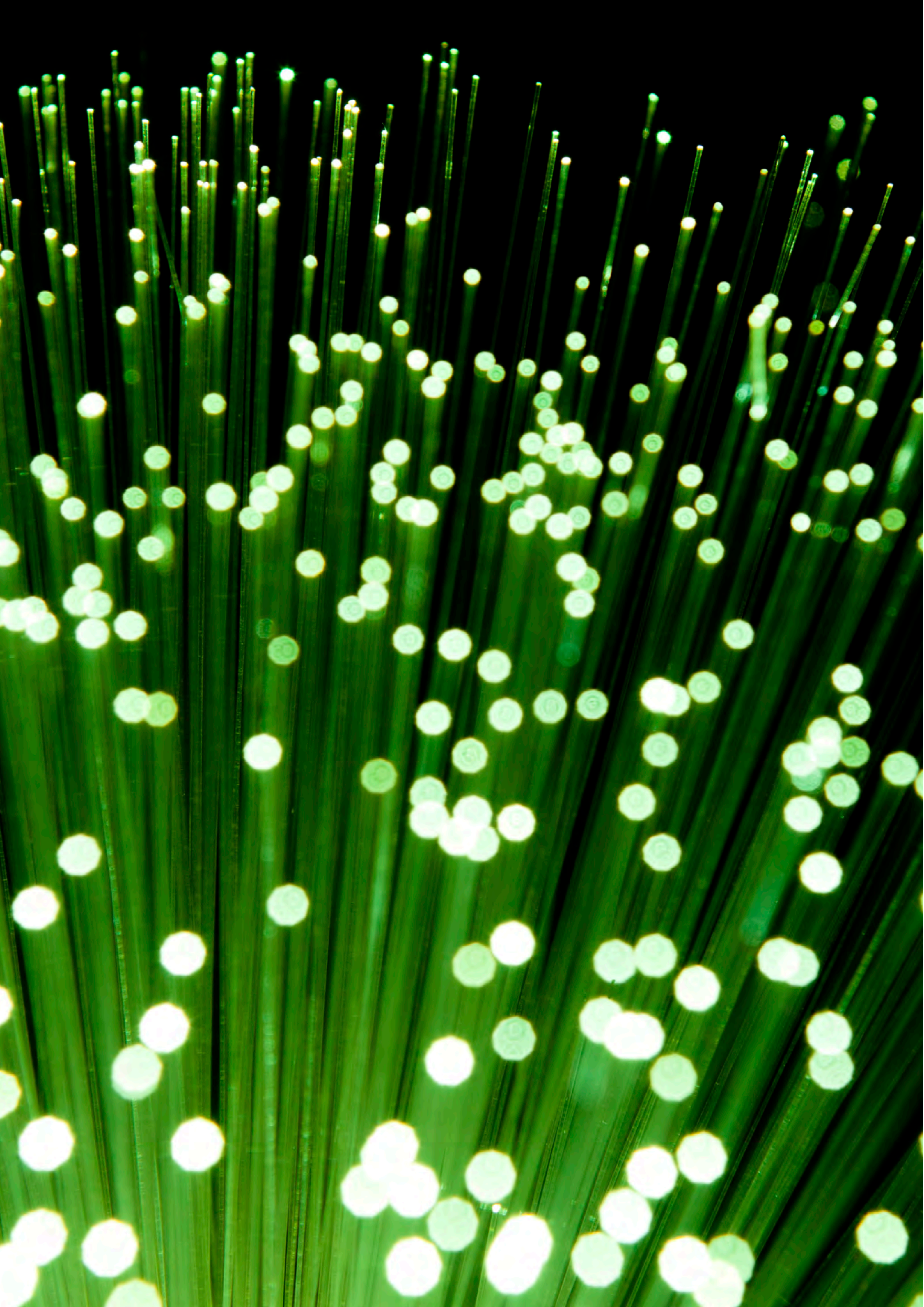
While all actors share the same objective of fostering a trusted and resilient cyberspace to fully reap the benefits of the hyperconnected world, capabilities vary regionally across the globe. Current challenges include: the lack of legal frameworks and mechanisms for international cooperation; disparities in cyber crime and privacy laws; differences in rules regarding extradition, legal procedures and evidence access and handling; and the inability to provide assistance to investigate and prosecute cyber criminals.

The discussions and workshops held over the last year have led us to the following recommendations:

- **For the private sector:**
  - Join the Partnering for Cyber Resilience initiative; commit to the Principles
  - Develop a pervasive culture of cyber awareness and resilience
  - Commit to responsibility and accountability for developing the organization’s level of cyber resilience
  - Promote the spread of best practices throughout supply chain
  - Engage in policy debate, and where possible, align under common core principles and commitments as a first step towards harmonizing policy needs
- **For the public sector:**
  - Work towards a flexible, but harmonized criminal justice capabilities framework
  - Engage private sector and adjacent policy domain experts to identify potential unintended consequences of policy development in advance
  - Ensure individual protections and foreign jurisdiction counterparts to share lessons learned and improve harmonization
  - For public agencies: join the Partnering for Cyber Resilience initiative; commit to the Principles
- **For the private and public sectors together:**
  - Commit to develop robust and sustainable public-private partnerships for a resilient cyber environment, based on clear and mutually agreed assignment of roles and responsibilities and the principle of accountability
  - Explore the need for the development of a cyber risk market
- **For academia:**
  - Promote the concept of economics of cyber security to non-specialist fields
  - Advance research on information sharing and the link between cyber resilience and national competitiveness

In the second year of the Risk and Responsibility in a Hyperconnected World project, the World Economic Forum will develop a tailored, capabilities-based set of guidelines for the basic legal and criminal justice components that governments should put in place to improve cyber resilience. The project will seek interaction with government representatives, both in policy development and policy enforcement communities, academics and business representatives in a series of workshops and interviews. This will contribute to developing guidelines for policy and criminal justice communities, and subsequently to seek support for this new initiative.

The interim results will be presented during the World Economic Forum Annual Meeting of New Champions 2012 in Tianjin, People’s Republic of China on 11-13 September.



Definitions

Cyber

"Cyber" refers to the interdependent network of information technology infrastructures, and includes technology "tools" such as the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

Cybersecurity

"Cybersecurity" refers to analysis, warning, information sharing, vulnerability reduction, risk mitigation and recovery efforts for networked information systems.

Cyber Risks

"Cyber risks" are defined as the combination of the probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation.

Cyber risks are a business issue with technical aspects. Cyber risk impacts and is impacted by all areas of the organization.

"Cyber threats" are potential cyber events that may cause unwanted outcomes, resulting in harm to a system or organization. Threats may originate externally or internally and may originate from individuals or organizations.

"Cyber vulnerabilities" are susceptibilities or insufficient defences in the protection of an asset or group of assets and capacities from cyber threats.

The primary **"values at risk"** from cyber threats and vulnerabilities are an entity's assets and reputation.

Cyber Risk Management

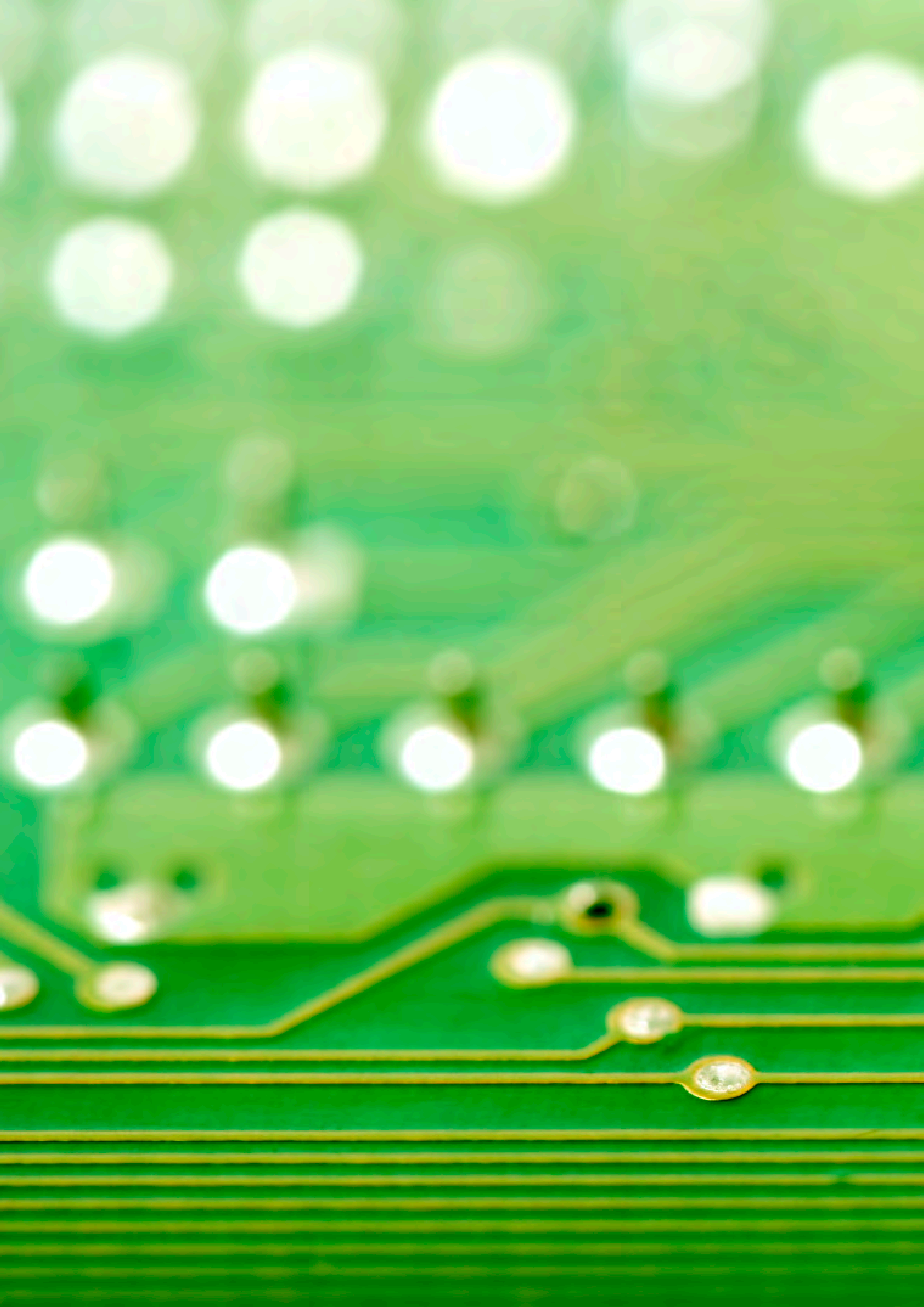
In addition to technical measures, cyber risk management seeks to influence human behaviour and norms, as well as technical controls and machine-to-machine interactions, and aims to coordinate activities and processes to prevent unwanted consequences.

A **"risk assessment"** is the process engaged in by an organization to analyse, evaluate and understand the spectrum of risks, their potential likelihood and their severity in order to enable it to act to mitigate unacceptable risk to the organization.

"Risk-transfer strategies" (such as indemnification, insurance and structured risk-transfer solutions) are ways for an organization to address risk.

Cyber Resilience

As an additional dimension of cyber risk management, **"cyber resilience"** is defined as the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery.

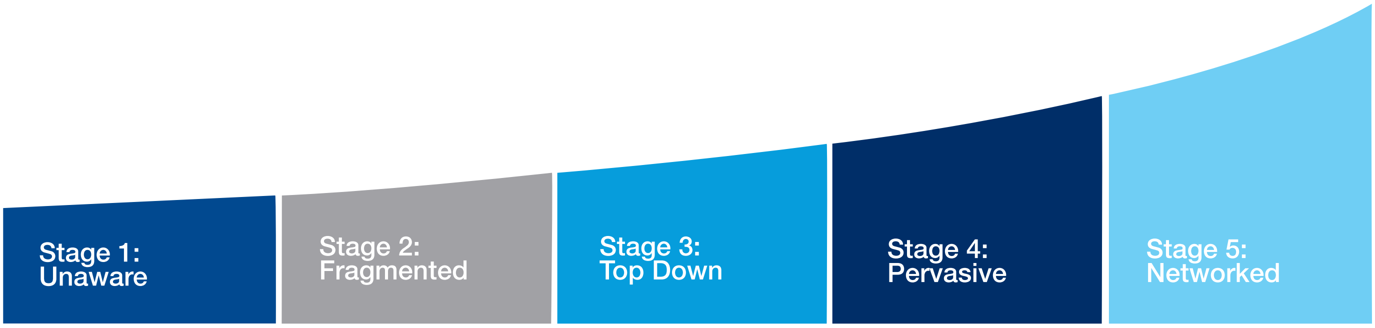


Appendix

The following section presents a checklist tool for chief executives and other C-suite executives to help guide their internal review of their organization’s cyber resilience capabilities. The tool is intended to provide executives with information to help inform their actions for the organization. It provides a rough composite score to locate the organization on a “hyperconnection readiness curve”. The questions asked in the tool can also help executives to identify specific strengths and weaknesses – and paths to improvement within their respective organization.

	1: Does not describe my organization at all 5: Accurately describes my organization					
Governance						
1.	The chief executive and executive management team are responsible for overseeing the development and confirming the implementation of a Programme of best practices for cyber risk management	1	2	3	4	5
2.	The chief executive and executive management team ensure that the Programme is reviewed for effectiveness and, when shortcomings are identified, corrective action is pursued	1	2	3	4	5
3.	The chief executive and the executive management team demonstrate visible and active commitment to the implementation of the Principles	1	2	3	4	5
4.	Executives and managers are responsible for understanding at the appropriate level how cyber risks could impact and originate from their line of business	1	2	3	4	5
5.	Senior leadership understands who is responsible for managing cyber risk when managing security incidents	1	2	3	4	5
6.	The organization has access to cyber expertise at its highest management levels	1	2	3	4	5
7.	The organization undertakes to continuously improve the integration of its cyber risk management with its other risk management initiatives	1	2	3	4	5
8.	The chief executive (or equivalent) has a clear decision path for action and communication in response to a significant security failure or accident	1	2	3	4	5
Programme						
9.	The organization conducts comprehensive assessments of its vulnerabilities to internal and external cyber risks appropriate for its industry and sector	1	2	3	4	5
10.	The organization monitors the effectiveness of its cyber risk management strategy	1	2	3	4	5
11.	The organization periodically internally verifies its compliance with rules and regulations	1	2	3	4	5
12.	The organization's commitment to the Programme is reflected in its policies and practices	1	2	3	4	5
13.	Managers, employees and agents receive specific training on the Programme, tailored to relevant needs and circumstances	1	2	3	4	5
14.	The organization has identified its data and information as vital assets, and organizes its Programme around the recognition that data and information have value that can be separately recognized and protected	1	2	3	4	5
15.	The risk management Programme includes all material third-party relationships and information flows	1	2	3	4	5
16.	The organization conducts comprehensive internal short- and long-term cyber risk impact assessments	1	2	3	4	5
Network						
17.	The organization seeks to ensure that its suppliers and relevant third parties adhere to the organization's specific cyber risk management standards or industry best practices, in line with the Principles, and formalizes this requirement using contractual obligations	1	2	3	4	5
18.	The organization has built relationships with its peers and partners to jointly manage cyber risk and more effectively deal with cyber incidents	1	2	3	4	5
19.	The risk management Programme includes all material third-party relationships and information flows	1	2	3	4	5
Average (gives maturity stage)						

The average score taken from the above check list provides an indication of overall cyber maturity as expressed in the stages in the chart below.



Stage 1: Unaware	Stage 2: Fragmented	Stage 3: Top Down	Stage 4: Pervasive	Stage 5: Networked
The organization sees cyber risk as largely irrelevant. Cyber risk does not form part of the organization's risk management process. The organization is not aware of its level of interconnectedness.	The organization recognizes hyperconnectivity as a potential source of risk, and has limited insight in its cyber risk management practices. The organization has a siloed approach to cyber risk, with fragmented and incidental reporting.	The chief executive officer has set the tone for cyber risk management, has initiated a top-down, risk response programme, but does not view cyber risk management as a competitive advantage.	The organization's leadership takes full ownership of cyber risk management, has developed policies and frameworks and has defined responsibilities and reporting mechanisms. Leadership understands the organization's vulnerabilities, controls and interdependencies with third parties.	Organizations are highly connected to their peers and partners, sharing information and jointly mitigating cyber risk as part of their day to day operations. Staff show exceptional cyber awareness and the organization is an industry leader in managing cyber risk management.

Endnotes

1. Internet World Stats, http://www.internetworldstats.com/stats.htm, 2011.
2. Cisco's Virtual Networking Index: Forecast and Methodology (2010-2015), http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf, 2011.
3. "CEO to shareholders: 50 billion connections 2020". Ericsson, http://www.ericsson.com/thecompany/press/releases/2010/04/1403231, 2010.
4. Bughin, J. and M. James. "Internet Matters: Essays in Digital Transformation". McKinsey Global Institute, http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Essays_in_digital_transformation, 2012.
5. New Resource – Lessons Learned from Ushahidi-Chile Earthquake Project." New Media Task Force. http://newmediataskforce.wordpress.com/2011/02/22/new-resource-lessons-learned-from-ushahidi-chile-earthquake-project, 2011.
6. Florencio, D. and C. Herley. Sex, Lies and Cyber Crime Surveys". Microsoft Research, https://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf.
7. Global Information Technology Report 2012. World Economic Forum.
8. Schneier, B. "Schneier on Security". http://www.schneier.com/blog/archives/2010/12/security_in_202.html, December 2010.
9. Sengupta, S. "Warned of an Attack on the Internet, and Getting Ready". The New York Times, http://www.nytimes.com/2012/03/31/technology/with-advance-warning-bracing-for-attack-on-internet-by-anonymous.html, 30 March 2012.
10. "Kaspersky Lab provides its insights on Stuxnet worm". Kaspersky Lab, http://www.kaspersky.com/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm, 2010.
11. Constantin, L. "Cyberterrorism Threat Shouldn't Be Underestimated, Some Security Experts Say". PCWorld, http://www.pcworld.com/article/251132/cyberterrorism_threat_shouldnt_be_underestimated_some_security_experts.
12. "National Strategy for Trusted Identities in Cyberspace". The White House, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf, April 2011.
13. MacIntosh, J. P., J. Reid and L. R. Tyler. "Cyber Doctrine: Towards a Coherent Evolutionary Framework for Learning Resilience". Institute for Security & Resilience Studies, 2011. p.71.
14. Supervisory Control and Data Acquisition SCADA networks are a category of software application programmes for process control and the gathering of data in real time from remote locations to control equipment and conditions. SCADA networks are used in power plants, oil and gas refining, telecommunications, transportation, and water and waste control systems.
15. "Blueprint for a Secure Cyber Future". US Department of Homeland Security, www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf, 2011.
16. "The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World". Government of the United Kingdom, https://update.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf, 2011.
17. An unrewarded risk is defined as a risk that, when incurred or accepted, has no potential positive benefit, but does have a potential negative result. As such, the risk is never "rewarded" positively and the actor has nothing to gain while indeed having something to lose.
18. Borg, S. "The Economics of Loss". Enterprise Information Security and Privacy, 2009.
19. DNSSEC: DNS Security Extensions Securing the Domain Name System, http://www.dnssec.net.
20. Moore, T. "The Economics of Cybersecurity: Principles and Policy Options". Center for Research on Computation and Society, Harvard University, 2010.
21. Moore, T. and R. Anderson. "Economics and Internet Security: A Survey of Recent Analytical, Empirical and Behavioral Research". Computer Science Group, Harvard University, 2011.
22. For an example, refer to http://www.cert.org/netsa/publications/faber-OARC2008.pdf
23. Anderson, R. and T. More. "Information Security Economics – and Beyond". Computer Laboratory, University of Cambridge, UK, 2007.
24. Segal, A. "Cyberspace Governance: The Next Step". Council on Foreign Relations, http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.
25. "Cyber Intelligence Sharing and Protection Act of 2011", http://intelligence.house.gov/bill/cyber-intelligence-sharing-and-protection-act-2011.
26. Gramm-Leach-Billey Act, http://www.ftc.gov/privacy/glbact/glbsub1.htm.

27. Mayerson, M. and D. Teshima. “Assessing the Risk of Cybercrime”. The Recorder, February 24, 2012.

28. Miller, M. “Is the long-term care insurance market sick?”, Reuters Money, November 19, 2010, http://blogs.reuters.com/reuters-money/2010/11/19/is-the-long-term-care-insurance-market-sick.

29. “Incentives and Challenges for Information Sharing in the Context of Network and Information Security”. European Network and Information Security Agency (ENISA), 2010, p.9.

30. “Sharing Information on Computer Systems Security: An Economic Analysis”,http://archive.nyu.edu/fda/bitstream/2451/15019/2/finalsbsio.pdf.

31. Cukier, K., V. Mayer-Schönberger and L.M. Branscomb. “Ensuring (and Insuring?) Critical Information Infrastructure Protection”. Faculty Research Working Papers Series, John F. Kennedy School of Government, Harvard University, 2005, http://belfercenter.ksg.harvard.edu/files/rwp_05_055_viktor_branscomb.pdf.

32. Ibid.

33. Ibid.

34. Industry Consortium for Advancement of Security on the Internet, www.icasi.org.

35. “Getting Ahead of Advanced Threats: Achieving Intelligence-Driven Information Security”. Security for Business Innovation Council, http://www.rsa.com/innovation/docs/CISO-RPT-0112.pdf.

36. Ibid.

37. Interview with Evangelos Ouzounis, Programme Manager of the Resilience and CIIP Programme, http://www.enisa.europa.eu/media/news-items/faqs-cyber-europe-2010-final.

38. “Information Sharing Practices That Can Benefit Critical Infrastructure Protection”. United States General Accounting Office,http://www.gao.gov/new.items/d0224.pdf, p.7.

39. “Incentives and Challenges for Information Sharing in the Context of Network and Information Security”. European Network and Infrastructure Security Agency, p.29.

40. “Information Sharing Practices That Can Benefit Critical Infrastructure Protection”. United States General Accounting Office; “Incentives and Challenges for Information Sharing in the Context of Network and Information Security”. European Network and Infrastructure Security Agency.

41. “Good Practice Guide on Information Sharing”. ENISA, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide.

42. “Information Sharing Practices That Can Benefit Critical Infrastructure Protection”. United States General Accounting Office, http://www.gao.gov/new.items/d0224.pdf, p.7.

43. Incentives and Challenges for Information Sharing in the Context of Network and Information Security”. European Network and Infrastructure Security Agency.

44. “Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing”. Information Technology Industry Council. p.7.

45. “Steps to Facilitate More Effective Information Sharing to Improve Cybersecurity”. Information Technology Industry Council, p.7.

46. Fontaine, R. And R. Will. “Internet Freedom: A Foreign Policy Imperative in the Digital Age”. Center for a New American Security, 2011.

47. “Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing”. Information Technology Industry Council.

48. Ibid.

49. Montalbano, E. “Federal Cyber Attacks Rose 39% in 2010”. InformationWeek, http://www.informationweek.com/news/government/security/229400156, 2011.

50. “Steps to Facilitate More Effective Information Sharing to Improve Cybersecurity”. Information Technology Industry Council, p.1.

51. Ibid; “Incentives and Challenges for Information Sharing in the Context of Network and Information Security”. European Network and Infrastructure Security Agency.

52. IT-ISAC 10 Year Anniversary, https://www.it-isac.org/IT-ISAC_MemberValueUpdatedJuly2011.pdf.

53. IT-ISAC, https://www.it-isac.org/about_n.php.

54. IT-ISAC 10 Year Anniversary, https://www.it-isac.org/IT-ISAC_MemberValueUpdatedJuly2011.pdf.

55. Ibid.

56. “Share Cyber Security Knowledge with Industry Leaders to Help Protect Your Company”. IT-ISAC, https://www.it-isac.org/files_n/IT-ISAC_Recruitment_Brochure.pdf.

Acknowledgements

The World Economic Forum's Risk and Responsibility in a Hyperconnected World is a global, multi-industry, multistakeholder project to improve cyber resilience, raise business standards and to contribute to a safer and stronger connected society. The project engages stakeholders across multiple industries and governments from around the world.

The project set out with the task of addressing global systemic risks arising from the hyperconnected environment in which information and communication technologies are driving across many areas of our societies and economies. The governance and strategic direction is guided by two core groups: a Steering Board and an Expert Working Group. This report is based on numerous discussions, workshops and research and the combined effort of all involved opinions expressed herein may not necessary correspond with each and every one involved with the project. The project intended to seek consensus among those participating.

Sincere thanks are extended to the industry experts who contributed their unique insights to this report. We are also very grateful for the generous commitment and support of Deloitte in their capacity as project adviser.

At the World Economic Forum, the energy and commitment of the report's editor and project lead, Derek O'Halloran, is to be acknowledged, as are Alan Marcus, Elsa Studer and Mark Schulman. Special thanks are also extended to Jolyon Barker, Alex de Leeuw and Peggy Brown of Deloitte whose insights were invaluable.

Steering Board

The Steering Board is responsible for strategic direction-setting as well as ensuring that the work produced is relevant and actionable at the highest level. As a lack of understanding about technology-driven risks is often cited as a risk in itself, the Steering Board members will be able to bring unified, clear and action-oriented voice to the wider debate in society.

Ian Livingston	Chief Executive Officer	BT Group
William E. McCracken	Chief Executive Officer	CA Technologies
Michael Chertoff	Senior of Counsel	Covington & Burling
Rob Wainwright	Director	Europol (European Police)
Natarajan Chandrasekaran	Chief Executive Officer and Managing Director	Tata Consultancy Services

Expert Working Group

The Expert Working Group brings together leading academic experts, thinkers and senior executives from IT and other industries. Executives cover the range of functional perspectives that need to be integrated in this topic, in particular risk, security and legal perspectives.

Steven R. Culp	Managing Director, Risk Management	Accenture
Eric Allegakoen	Vice-President, Global Audit and Assurance Services	Adobe Systems
William J. Casazza	Senior Vice-President and General Counsel	Aetna
Mark Walsh	Vice-President, Information Security	BAE Systems
Susan Kish	Head of Cross-Platform Initiatives	Bloomberg
Allan Friedman	Research Director, Center for Technology Innovation	Brookings Institution
Ray Stanton	Global Head of Business Continuity, Security and Governance	BT Group
Phillip Harrington	Executive Vice-President, Risk, and Chief Administrative Officer	CA Technologies
Meghan McAuley Hannes	Managing Director	CloudInsure
Drew Bartkiewicz	Chief Executive Officer	CyberFactors
Kevin Harried	Senior Vice-President, Director of Risk Management	FIS
Mustaque Ahamad	Director, Information Security Center	Georgia Institute of Technology
Jody Westby	Chief Executive Officer	Global Cyber Risk
Mohd Noor Amin	Chairman	Impact
Andrew Vitrano	Vice President, Deputy General Counsel	IntraLinks Holdings
Mark Bauhaus	Executive Vice-President and General Manager, Service, Support and Operations	Juniper Networks
Scott David	Executive Director of the Law, Technology & Arts Group	University of Washington Law School
Christophe Nicolas	Senior Vice-President, Head of Cyber Services and Technologies	Kudelski Group
John D. Evans	Vice-President, International Initiatives	Lockheed Martin Corporation
Ray Johnson	Senior Vice-President and Chief Technology Officer	Lockheed Martin Corporation
Cristin Goodwin	Senior Attorney	Microsoft Corporation
Serge Dumont	Group Vice-Chairman and Chairman, Asia Pacific	Omnicom Group
Owen Tripp	Chief Operating Officer	Reputation.com
Bret Hartman	Chief Technology Officer	RSA
JP Rangaswami	Chief Scientist	Salesforce.com
Yuecel Karabulut	Chief Security Adviser	SAP Labs
Marc Goodman	Faculty Member and Security Adviser	Singularity University
Anwarul Hasan	Director, Risk Management	Swiss Reinsurance Company
David Kirkpatrick	Founder and Chief Executive Officer	Techonomy Media
Deirdre Stanley	Executive Vice-President and General Counsel	Thomson Reuters
Murat Sonmez	Executive Vice-President, Global Field Operations	TIBCO Software
Julian Sevillano	Global Head, Enterprise Risk Management	Visa
Alexis Samuel	Chief Risk Officer	Wipro Limited
Tarkan Maner	President and Chief Executive Officer	Dell Wyse

Additional Advisers

Lee Hibbard	Secretary, Cybercrime Convention Committee and Head of Data Protection and Cybercrime, Directorate-General of Human Rights and Rule of Law	Council of Europe
Paul L. Saffo	Author and Forecaster	Discern Analytics
Peter Hustinx	Supervisor	European Data Protection
Stacy Feuer	Assistant Director for International Consumer Protection	Federal Trade Commission
Jonathan Zittrain	Professor of Law and Professor of Computer Science	Harvard University
Rod A. Beckstrom	President and Chief Executive Officer	ICANN
Hamadoun I. Touré	Secretary-General	International Telecommunication Union (ITU)
Jun Murai	Dean and Professor, Faculty of Environment and Information Studies	Keio University
Atsushi Umino	Director for International Policy Coordination, Global ICT Strategy Bureau	Ministry of Internal Affairs and Communications of Japan
Viktor Mayer-Schönberger	Professor, Internet Governance and Regulation	Oxford Internet Institute
Michael Fertik	Founder and Chief Executive Officer	Reputation.com
Robert Kirkpatrick	Director, UN Global Pulse, Executive Office of the Secretary-General	United Nations
Colin Adams	Director of Commercialisation, School of Informatics	University of Edinburgh
Ken Senser	Senior Vice-President, Global Security, Aviation and Travel	Wal-Mart Stores

Project Adviser: Deloitte

Jolyon Barker, Lead Adviser	Managing Director, Global Technology, Media and Telecommunications	Deloitte UK
Jacques Buith	Managing Partner, Global TMT Leader Enterprise Risk Services	Deloitte The Netherlands
Simon Owen	Managing Partner, Enterprise Risk Services - EMEA	Deloitte UK
JR Reagan	Principal, Federal Chief Innovation Officer	Deloitte USA

Contacts

Alan Marcus, Senior Director
Head of Information Technology
and Telecommunications Industries
World Economic Forum

alan.marcus@weforum.org

Derek O'Halloran, Global Leadership Fellow
Information Technology Partnerships
World Economic Forum

derek.ohalloran@weforum.org

Alex de Leeuw, Project Manager
Information Technology Partnerships
World Economic Forum

alex.deleeuw@weforum.org

Elsa Studer, Community Associate
Information Technology and North America
World Economic Forum

elsa.studer@weforum.org

www.weforum.org/cyber

cyberresilience@weforum.org

WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum is an independent international organization committed to improving the state of the world by engaging business, political, academic and other leaders of society to shape global, regional and industry agendas.

Incorporated as a not-for-profit foundation in 1971 and headquartered in Geneva, Switzerland, the Forum is tied to no political, partisan or national interests.

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