WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Advancing Cyber Resilience: Project Scoping Workshop

Location: World Economic Forum USA offices (3 East 54th Street, 18th Floor, New York, NY 10022)
19 November 2015

Background Materials

***Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World – Principles and Guidelines* (March 2012)** (PDF)

Pathways to Global Cyber Resilience (2012) (PDF)

***Risk and Responsibility in a Hyperconnected World* (January 2014)** (PDF)

***Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats* (January 2015)** (PDF)

Project History

In recognition of the risks and rewards of the networked economy and how and fundamental for sustainable growth and stability digital technologies have become, the World Economic Forum has engaged with these issues as part of its global agenda. The Cyber Resilience programme arose from this broader work as only a coordinated approach can ensure that new opportunities for growth are fully leveraged while the risks that come with them are effectively managed.

The initiative started at the World Economic Forum Annual Meeting 2011 in Davos when the Forum and its community of public and private sector organizations launched a multistakeholder project to address global systemic risks arising from the growing digital connectivity of people, processes and infrastructure.

In the first year of the Cyber Resilience project, CEOs and top-level organization leaders agreed to the Principles for Cyber Resilience. These core principles of the Forum's Partnering for Cyber Resilience initiative were established to raise awareness of cyber risk and to build commitment regarding the need for more rigorous approaches to cyber risk mitigation. The core principals are:

1. Recognition of interdependence
   - All parties have a shared interest in fostering a common, resilient digital ecosystem
2. Role of leadership
   - Encourage executive-level awareness and leadership of cyber risk management
3. Integrated risk management
   - Develop a practical and effective implementation programme that aligns with existing frameworks
4. Promote uptake
   - Encourage suppliers and customers alike to develop similar levels of awareness and commitment

These Principles are memorialized in the Forum's publications: *Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World – Principles and Guidelines,* expanded in *Pathways to Global Cyber Resilience*.

A series of workshops organized around the Principles and Guidelines for Cyber Resilience advanced discussion to produce valuable guidelines and best practice principles for chief executives and government leaders. While the initial focus was on raising senior leader-level awareness of – and attention to – cyber resilience, the initiative also recognized the need for shared cyber resilience assurance benchmarks across industries and domains.

Toward that end, the project developed a cyber-risk framework to improve cyber resilience of individual organizations, with critical components for organizations to consider, including existing threats, vulnerabilities, value-at-risk and potential responses.

The project also conducted a study on global macro impact of cyber threats (up to $3tr/5% global GDP by 2020), future scenarios, and developed a *Framework for Global Collaboration*.

This work is more fully described in the Forum's publications: *Risk and Responsibility in a Hyperconnected World* and *Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats*.

As this work progressed, the Forum and its partners recognized that several areas require further exploration: cyber-crime, new networked technologies (like the Internet of Things), industry-specific risk analyses, and a continuing assessment of risk normalization.

Cyber Resilience within the World Economic Forum

The emergence of the internet and networked technologies as a key driver of the Fourth Industrial Revolution demanded a multi-faceted response from the Forum and its stakeholders. The ICT industry was naturally, both in the Forum and the wider world, the first locus of activity relating to digital transformation and security. As the impact of these technologies has spread, however, all actors in the economy and society are increasingly working together to reap the benefits and mitigate the risks of these technologies.

Within the Forum, this recognition of the necessity for a multi-stakeholder response prompted the development of the Future of the Internet Initiative (FII). This initiative has five main pillars, one of which, Cyber Crime, is a component of Cyber Resilience. As a practical matter, however, cyber-crime is sufficiently distinct and expansive that a separate project is merited. The Cyber Crime project is therefore dedicated to ensuring cooperation between criminal justice agencies and relevant stakeholders in order to develop practical measures for combatting cybercrime and prioritize cyber-specific legislation.

Cyber Resilience continues as a Forum project that examines the risks of networked technologies beyond the criminal justice frame. This work will include the industry-specific risk analyses and examinations of the risk profile of new technologies, which have been identified as key priorities by project members, as well as other industry-led areas of inquiry, such as risk normalization, to be developed during our scoping phase.

Other “Cyber” Work	Cyber Resilience Project
Crime or Espionage Frame	Business Strategy Frame
Government Entities are main actors	Business and Industry are main actors
Information Technology (IT) focus	IT *and* Operational Technology (Including IOT)
Views cyber risk in the aggregate	Particularizes risks industry-by-industry

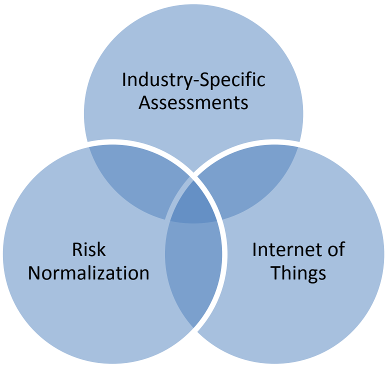
Advancing Cyber Resilience

Thanks in part to the Forum’s Partnering for Cyber Resilience initiative and the widespread promulgation of the Principles and the Guidelines, the conversation surrounding cybersecurity has matured among top-level leaders from generalizations to a more clear understanding of threats to networks and organizations. The quantification of these risks must likewise become more sophisticated and granular in order to support the decisions that business strategists and policy makers must make to support the digital economy.

The current stage of this project, Advancing Cyber Resilience, aims to continue the work of the Partnership while advancing thinking in the area of cyber security and resilience. The examination of risk according to industry group is an important step in the creation of an understanding of the commonalities and differentiations cybersecurity risk across industries and even within enterprises.

This quantification of cybersecurity risk allows for the normalization of these risks so that leaders can better determine business strategy, given that these risks exist. A further goal of normalization is to allow for the availability of mechanisms to alleviate or respond to cyber risks and other risk mitigation tools for organizations to ensure the resilience of their increasingly digital business functions.

This examination, in the past, has been conducted almost exclusively in relation to information security. The emergence of new networked technologies that may only incidentally involve human interaction, such as the Internet of Things, forces an expansion of the scope of risk examinations beyond data to networks, infrastructure, and virtually every component of industry and society. In developing the scope of the current project, the ramifications of these innovations will be closely examined.



Just as the Partnership for Cyber Resilience helped to raise awareness and prompt action in the face of the emergence of cyber security risk, the current project will improve our understanding of where, exactly these risks originate (in terms of technology), to whom these risks accrue (which industries), and how these risk can be evaluated as part of firms’ strategic planning. The scope and priority of these overlapping inquiries is the first step in creating digital enterprises that are more aware of the precise nature of the threats they face and, ultimately, more resilient.