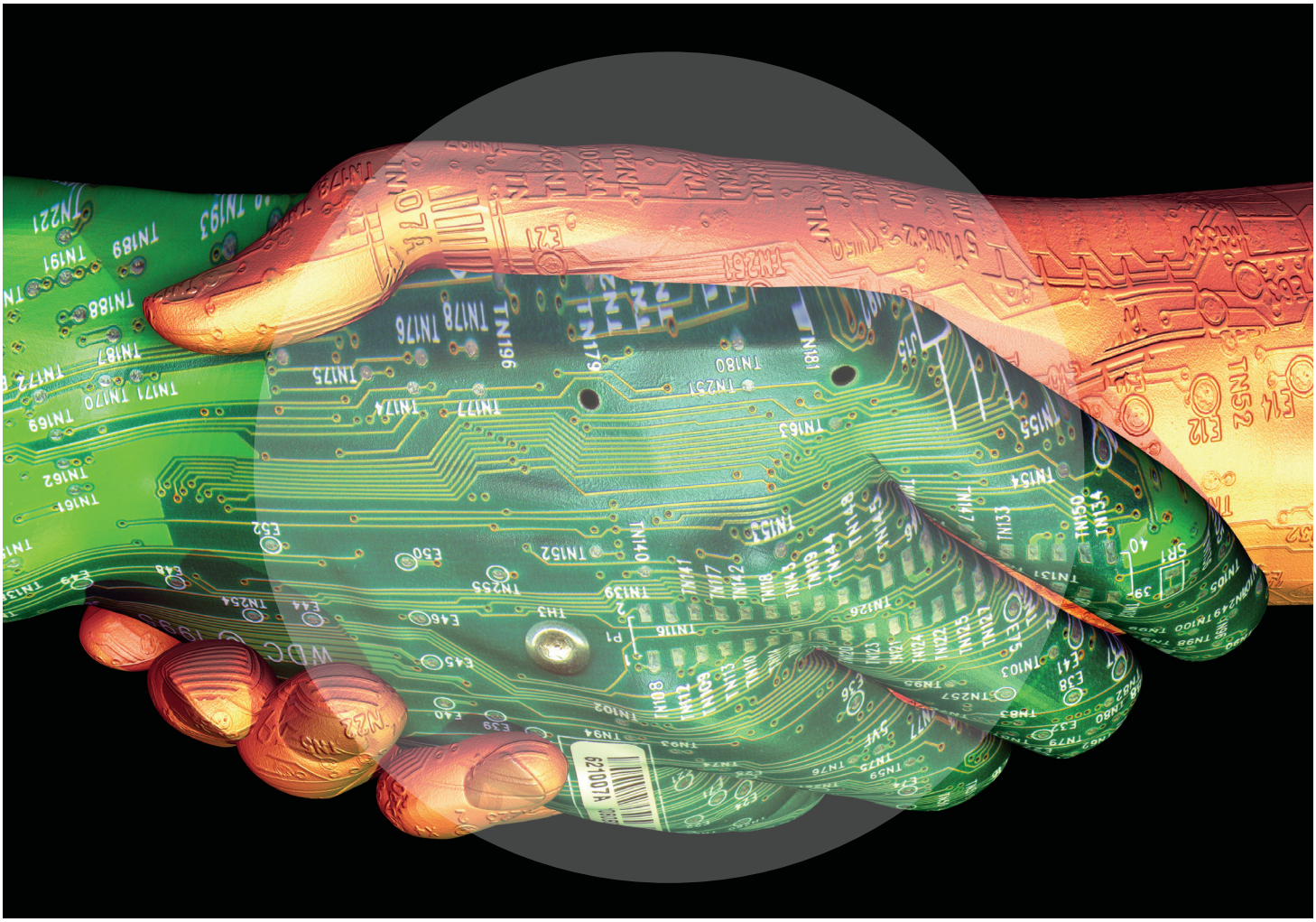
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Partnering for Cyber Resilience

Risk and Responsibility in a Hyperconnected World - Principles and Guidelines

March 2012



This document was created through a collaborative process with multiple partners.
Special thanks go to Project Advisers Deloitte.

© World Economic Forum

2012 - All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means,
including photocopying and recording, or by any information storage and retrieval system.

REF 270912

Contents

Introduction

The World Economic Forum recognizes that the risks, rewards and governance of the networked economy are core issues of the global agenda and fundamental for sustainable growth and stability. Additionally, it recognizes that only a coordinated approach will ensure that new opportunities for growth are fully leveraged and risks managed.

Throughout 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. Some simple observations about the rapidly evolving environment can guide us in developing an appropriate response.

- Increasing dependence on connectivity for the normal functioning of society makes the protection of connectivity a critical issue for all; as a shared resource like clean air or water, the challenge is defined as one of interdependence
  - No one organization can resolve the issue by itself and 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 cyber risk landscape evolves rapidly: defensive strategies mean we are always fighting the last battle, and there are many "unknown unknowns"
  - Solutions that focus on specifics will be outdated rapidly; a principle-based approach is required

- The free flow of information must continue to drive economic value; a locked down economy is a frozen economy
  - Resilience, not just bigger locks, is the goal; accepting that failures will occur, the objective is to restore normal operations and ensure that assets and reputations are protected

- The primary vulnerability of many organizations is human – awareness, leadership and execution
  - The role of leadership is to set the structure and tone; simple practices can dramatically improve an organization's risk profile

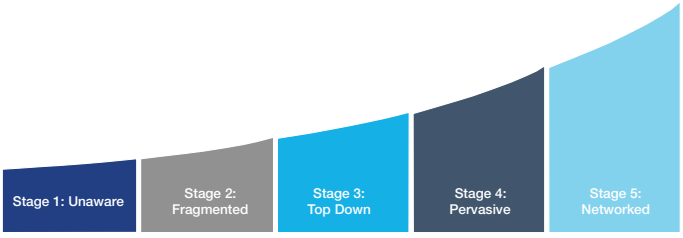
As such, the objective of this initiative is to seek commitment to a common set of shared principles for leadership – shifting mindsets from just securing perimeters to also including a focus on interdependence and resilience.

These principles are aimed at all organizations, regardless of industry, sector, jurisdiction, geography or level of current expertise. They are intended to be non-prescriptive, as context will vary. They are based on simple organizational good practices and a recognition of the distributed nature of the challenge.

The principles are supported by a set of guidelines to which organizations can refer to help develop their own responses. A simple maturity model and definition of terms is also provided for common reference.

Figure 1: Maturity Model for Organizational Cyber Resilience

Maturity Model



1. Commitment to Cyber Resilience

We, the undersigned, support the multi-industry, multinational and multistakeholder initiative and principles to improve systemic resilience to cyber risks.

The widespread adoption of these principles is intended to help raise business standards associated with hyperconnected information systems across the world and contribute to the shared goals of economic stability and prosperity.

We collectively recognize the interdependence of private and public sector organizations in the global, hyperconnected environment. As such, we recognize our role in contributing to the overall levels of cyber risk mitigation on a national and global level.

We support the Principles for Cyber Resilience ("Principles"), derived from multistakeholder dialogue across multiple regions and sectors. The Principles (detailed further below) are:

1. Recognition of interdependence: All parties have a role in fostering a resilient shared digital space

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

4. Promote uptake: Where appropriate, encourage suppliers and customers to develop a similar level of awareness and commitment

With this signature, we commit to these Principles in support of creating and maintaining a resilient online environment and a network of mutually trusted entities.

We therefore support and call for broad support of this initiative.

Name (print): _____

Position: _____

Company: _____

Date: _____

Signature: _____

2. Principles for Cyber Resilience

2.1 The organization recognizes the interdependent nature of our hyperconnected world and its own role in contributing to a safe shared digital environment

We are all only as strong as the weakest link in the chains upon which we all depend; we each contribute to the safety of our hyperconnected world. An open, secure and resilient online space is a public good; all actors share responsibility for creating and supporting this resource.

2.2 The executive management team recognizes its leadership role in setting the tone and structure for cyber resilience

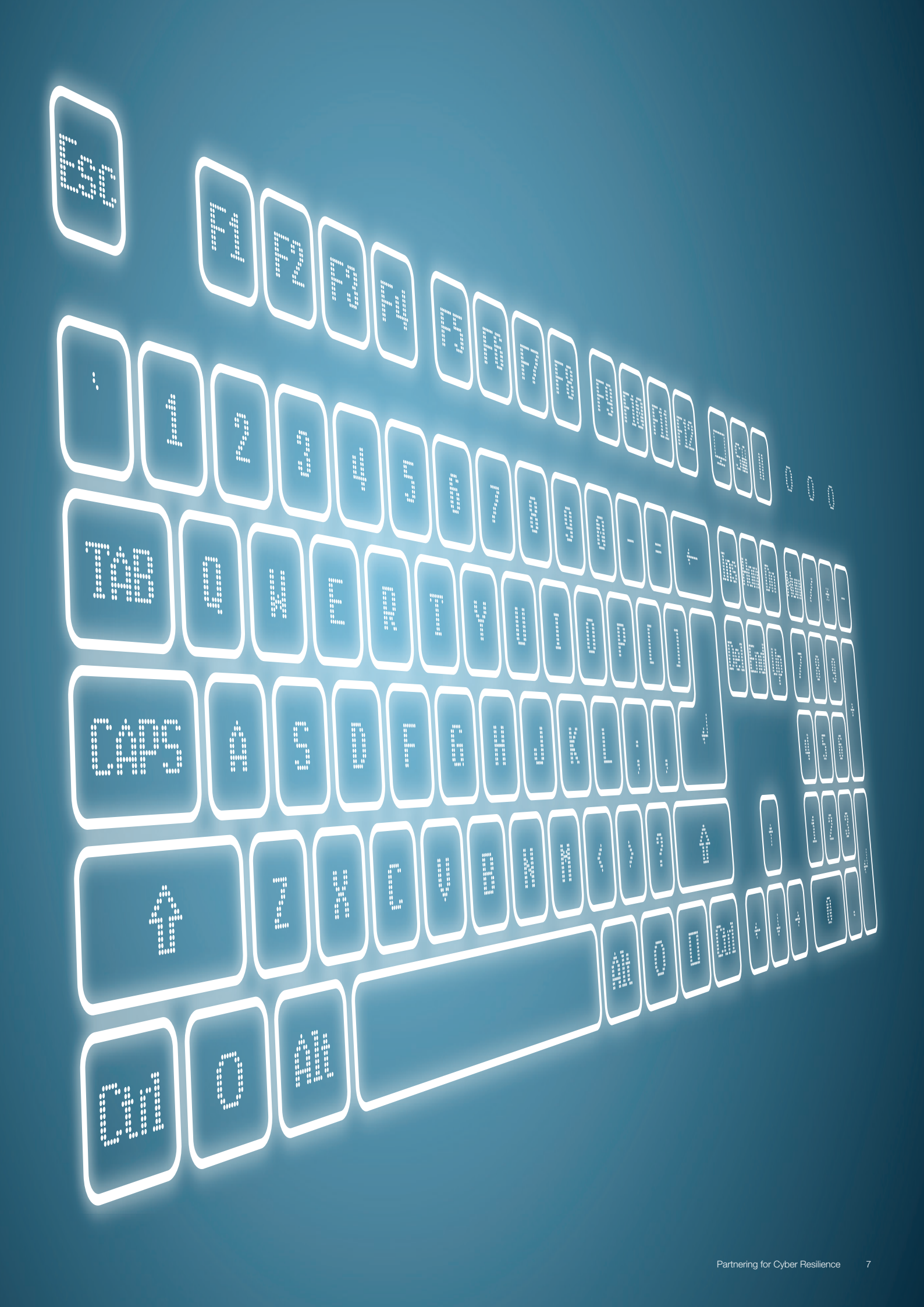
In line with its fiduciary and other leadership duties, the executive leadership recognizes the important nature of mitigating cyber-related risks as an essential element of the on-going viability and success of their institution, safeguarding its intellectual property and protecting the information it holds in order to deliver products or services to its customer or constituent base, consistent with the applicable sector and jurisdiction law.

2.3 The organization recognizes the importance of integrating cyber risk management within its broader risk practices and in line with these Principles and Guidelines

Consistent with sector and jurisdiction-applicable uniform good information practices now or hereafter in effect, a specific programme geared towards managing known cyber risks should be continuously pursued by the entity that can take account of guidance and standards relevant to the sectors and regions in which it operates. In doing so, it reduces the risk of harm to itself, positively contributes to the resilience of the connected information environments in which it operates and demonstrates good (corporate) citizenship.

2.4 The organization encourages its suppliers to adopt these Principles and Guidelines

In recognition that widespread adoption of these Principles contributes to the continued and enhanced opportunity for all stakeholders to benefit from hyperconnectivity, and to more effectively secure supply chains and manage the interdependence and vulnerability that this connectivity entails, the organization should leverage its relationships to encourage others to adopt the Principles.



3. Guidelines for Cyber Resilience: Programme Development

This section defines a set of capabilities that enterprises should aspire to meet, at a minimum, when implementing their own cyber risk management programme ("Programme"). The items below are intended as non-prescriptive guidance on the capabilities that any such effective Programme should include, and may describe practices that are already in place. Specific standards, processes and legal requirements will vary by industry and jurisdiction and may change over time, and specific instances of a relevant Programme will be informed by such context.

3.1 Starting Assumptions

3.1.1 The interdependence of all organizations within the online environment provides a foundational assumption for all cyber risk management.

3.1.2 Improving cyber risk management practices within a single organization contributes to global cyber resilience.

3.1.3 A risk-based approach is an efficient and effective approach to deal with cyberthreats.

3.1.4 Recognizing that 100% risk mitigation is not possible in any complex system, the overarching goal of a risk-based approach to cybersecurity is system resilience to survive and quickly recover from attacks and accidents.

3.2 Governance: Leadership and Tone

3.2.1 The executive management team is accountable for overseeing the development and implementation of an effective programme of best practices for cyber risk management within its broader risk management activities.

3.2.1.1 The Programme should be based on the Principles and other relevant company priorities, and the executive management team should provide leadership, resources and active support for the implementation of the Programme.

3.2.1.2 The executive management team ensures that the Programme is internally reviewed for effectiveness and, when shortcomings are identified, corrective action is taken.

3.2.2 The Chief Executive Officer (or equivalent) and the executive management team demonstrates visible and active commitment to the implementation of the Principles.

3.2.3 The Chief Executive Officer (or equivalent) is ultimately resonsible for consistently carrying out the Programme with clear lines of authority, accountability, delegation and responsibility.

3.2.4 Executives and managers are provided with the tools and authority to promote resilience, and mitigate cyber risks that could impact and/or originate from their respective lines of business, and otherwise perform their responsibilities for the organization in a way that is consistent with the Principles.

3.2.5 The Chief Executive Officer (or equivalent) has a clear plan and decision path for action and communication in the event of a significant failure of networked information systems provided or used by the organization.

3.3 Programme Implementation: Critical Operational Components

3.3.1 The concepts and elements of the Programme are integrated into the overall enterprise risk management programme where relevant.

3.3.2 The Programme includes a mechanism to assess and monitor cyber risk.

3.3.2.1 The Programme forms part of the organization's on-going risk management practices and includes policies that are intended for identifying, assessing, measuring, prioritizing, monitoring, mitigating and transferring cyber risk, applying existing best practices or guidelines where possible.

3.3.2.2 The Programme includes internal impact assessments on operations, assets and reputation in both qualitative and quantitative (financial) terms.

3.3.2.3 The Programme includes specific strategies that are intended to reduce mean time to recovery (i.e. improve resilience) in the event of major attacks or failures.

3.3.2.4 The organization monitors the effectiveness of improving cyber resilience and reducing cyber risk.

3.3.2.5 The organization regularly evaluates and ensures that it allocates adequate resources to its risk management strategy.

3.3.3 The organization periodically internally verifies its compliance with applicable rules and regulations that are relevant for its cyber risk exposure.

3.3.4 The organization's practices and policies incorporate and reflect its commitment to improving cyber resilience and reducing risk.

3.4 Suppliers and Third Parties

3.4.1 The organization ensures that parties that are not directly subject to internal company policies – but the behaviour of which is made reliable by contract including 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 formalize this requirement using such contractual obligations.

3.4.2 Where appropriate, contractors and suppliers should receive training in the Programme.

4. C-Suite Executive Checklist

The following section presents a simple 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 both general and specific information to help inform their actions for the organization. It provides a rough composite score to locate the organization on a "hyperconnection readiness curve" set forth below. The questions asked in the tool can also help executives to identify specific strengths and weaknesses – and paths to improvement within their respective organization.

Note: Because of the subjectivity of evaluation from one entity to another, and the current absence of metrics for each of the variables below, the benchmarking is not intended for use in comparing the Programme of one entity against another, nor the conformity of a particular Programme against any external norms or rules.

		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)						

Maturity Model

Stage 1: Unaware

The organization sees cyber risk as largely irrelevant, and cyber risk does not form part of the organization's risk management process. The organization is not aware of its level of interconnectedness.

Stage 2: Fragmented

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.

Stage 3: Top Down

The Chief Executive Officer has set the tone for cyber risk management, has initiated a top-down threat-risk-response program but does not view cyber risk management as a competitive advantage.

Stage 4: Pervasive

The organization's leadership takes full ownership of cyber risk management, has developed policies and frameworks, and has defined responsibilities and reporting mechanisms. It understands the organization's vulnerabilities, controls, and interdependencies with third parties.

Stage 5: Networked

Organizations are highly connected to their peers and partners, sharing information and jointly mitigating cyber risk as part of their day-to-day operations. Its people show exceptional cyberawareness and the organization is an industry leader in managing cyber risk management.

5. Programme Development: Scope and Definitions

This initiative takes an “act locally, think globally” approach. It focuses on the improvement of the local cyber resilience of individual organizations. Through coordination on common principles, these local actions create global benefits. Common principles leverage the effectiveness of individual organizations’ actions into a cohesive community of cyber resilience.

A critical roadblock to shared understanding and to resolving any challenge is differences in interpretation of the scope and terms that define the issue. This section sets out definitions and describes some of the terms used above that are relevant in designing, developing and deploying solutions for cyber risk under the Principles.

5.1 Cyber

5.1.1 "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.

5.2 Cybersecurity

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

5.3 Cyber Risks

5.3.1 "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.

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

5.3.3 "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.

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

5.3.5 The primary "values at risk" from cyber threats and vulnerabilities are an entity's assets and reputation. Because of critical dependencies, the consequences on these assets could be the result of a larger, cascading event beyond the entity's direction or control.

5.4 Cyber Risk Management

5.4.1 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.

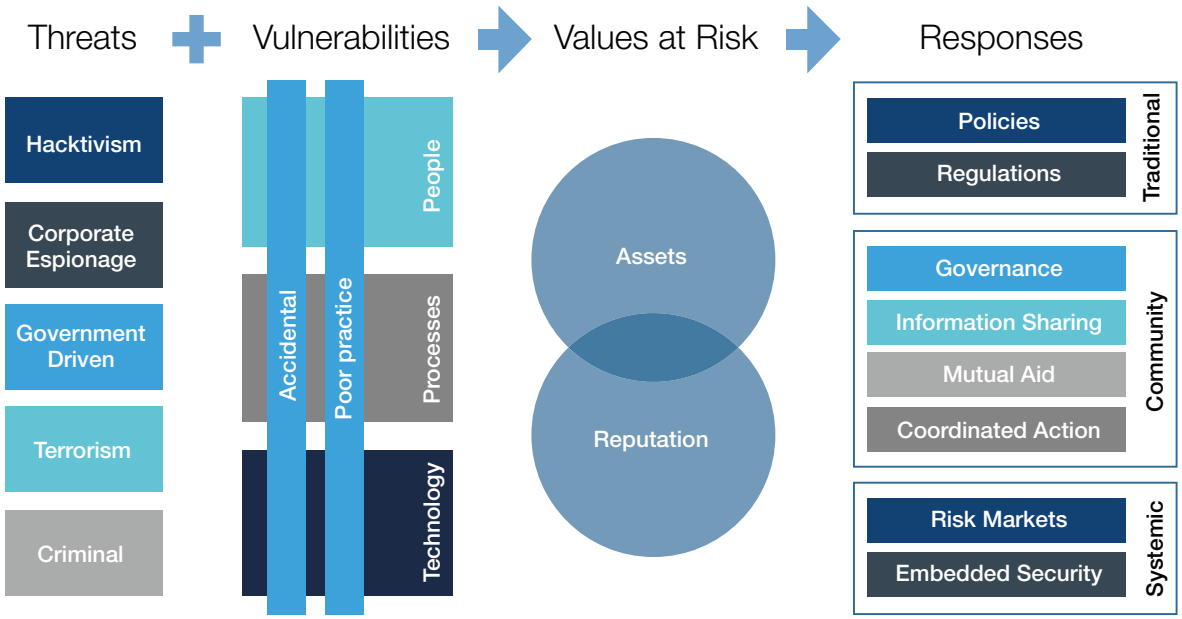
5.4.2 A "risk assessment" is the process engaged in by an organization to analyse, evaluate and understand the spectrum of risks, their potential likelihood and their severity in order to enable it to act to mitigate unacceptable risk to the organization.

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

5.5 Cyber Resilience

5.5.1 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.

Figure 2: Cyber Risk Framework



Acknowledgements

Steering Board

Natarajan Chandrasekaran	Chief Executive Officer and Managing Director	Tata Consultancy Services
Michael Chertoff	Co-Founder and Managing Principal	Chertoff Group
Ian Livingston	Chief Executive Officer	BT Group
William E. McCracken	Chief Executive Officer	CA Technologies
Robert Wainwright	Director	Europol (European Police)

Working Group

Mustaque Ahamad	Professor and Director	Georgia Tech Information Security Center
Eric Allegakoen	Vice-President, Global Audit and Assurance Services	Adobe
Mohd Amin	Chairman	Impact
Jolyon Barker	Managing Director, Global Technology, Media and Telecommunications	Deloitte (Project Adviser)
Drew Bartkiewicz	Vice-President, Strategy Services	Mashery
Mark Bauhaus	Executive Vice-President and General Manager	Juniper Networks
Jennifer Byrne	Vice-President	Lockheed Martin
William Casazza	Senior Vice-President and General Counsel	Aetna
Paloma Castro	Director, Global Corporate Affairs	LVMH
Steve Culp	Managing Director, Risk Management	Accenture
Scott David	Partner (OIX Legal Counsel)	K&L Gates
Serge Dumont	Group Vice-Chairman and Chairman, Asia Pacific	Omnicom
John Evans	Vice-President, Business Innovation	Lockheed Martin
Stacy Feuer	Associate Director for International Consumer Protection	Federal Trade Commission
Allan Friedman	Research Director, Center for Technology Innovation	Brookings Institution
Marc Goodman	Faculty Member and Security Adviser	Singularity University
Cristin Goodwin	Senior Attorney	Microsoft Corporation
Meghan Hannes	Managing Director	CloudInsure
Kevin Harried	Senior Vice-President, Risk Management	FIS/Capco
Phillip Harrington	Executive Vice-President, Risk, and Chief Administrative Officer	CA Technologies
Bret Hartman	Chief Technology Officer, RSA	EMC
Anwarul Hasan	Director, Risk Management	SwissRe
Ray Johnson	Senior Vice-President and Chief Technology Officer	Lockheed Martin
Yuecel Karabulut	Chief Security Adviser	SAP
David Kirkpatrick	Founder and Chief Executive Officer	Techonomy
Robert Kirkpatrick	Director	UN Global Pulse
Susan Kish	Head of Cross-industry Platforms	Bloomberg
Tarkan Maner	President and Chief Executive Officer	Dell Wyse
Christophe Nicolas	Senior Vice-President and Chief Technology Officer	Kudelski Group
JP Rangaswami	Chief Scientist	Salesforce.com
Paul Saffo	Author and Forecaster	Discern Analytics
Alexis Samuel	Chief Risk Officer	Wipro
Murat Sonmez	Executive Vice-President, Global Field Operations	TIBCO Software
Deirdre Stanley	General Counsel	Thomson Reuters
Ray Stanton	Global Head of Business Continuity, Security and Governance	BT Group
Owen Tripp	Chief Operating Officer	Reputation.com
Andrew Vitrano	Associate General Counsel and Assistant Corporate Secretary	IntraLinks
Mark Walsh	Vice-President, Information Security	BAE Systems
Jody Westby	Chief Executive Officer	Global Cyber Risk

Additional Advisers

Colin Adams	Director of Commercialisation, School of Informatics	University of Edinburgh
Rod Beckstrom	Chief Executive Officer	ICANN
Michael Fertik	Founder and Chief Executive Officer	Reputation.com
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
Peter Hustinx	Supervisor	European Data Protection
Viktor Mayer-Schönberger	Professor, Internet Governance and Regulation	Oxford Internet Institute
Jun Murai	Dean and Professor, Faculty of Environment and Information Studies	Keio University
Ken Senser	Senior Vice-President of Global Security, Aviation and Travel	Wal-Mart
Hamadoun I. Touré	Secretary-General	International Telecommunication Union (ITU)
Atsushi Umino	Director for International Policy Coordination, Global ICT Strategy Bureau	Ministry of Internal Affairs and Communications
Jonathan Zittrain	Professor of Law and Professor of Computer Science	Harvard University

Contact: Derek O'Halloran, Global Leadership Fellow Information Technology Partnerships, World Economic Forum, derek.ohalloran@weforum.org
Alex de Leeuw, Information Technology Partnerships, World Economic Forum, alex.deleeuw@weforum.org
Elena Kvochko, Information Technology Partnerships, World Economic Forum, elena.kvochko@weforum.org
www.weforum.org/cyber

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