WORLD ECONOMIC FORUM

Systemic Cybersecurity Risk and role of the Global Community: Managing the Unmanageable

BRIEFING PAPER

NOVEMBER 2022

Images: Getty Images

Contents

Systemic cyber risk

Cyberattacks are frequently becoming 'cyber events' with systemic impact. How can governments and businesses respond?

In February 2022, a cyberattack on commercial satellite services in Ukraine caused electricity-generating wind farms to shut down across Central Europe. In July 2021, supermarkets in Sweden were forced to close their doors after a cyberattack on an IT services provider based in Florida, USA. In both cases, the rolling flow of disruption was neither predicted nor predictable. These incidents show how the technologies that support businesses, infrastructure and societies are increasingly interdependent, and vulnerable.

Different technologies across a multitude of organizations now have the same common dependencies or weaknesses. This means the impact of cybersecurity incidents can cascade from organization to organization and across borders. The risks this creates are systemic, contagious and often beyond the understanding or control of any single entity. Systemic risks can be difficult to predict and quantify, and even more difficult to manage.

Traditional cybersecurity approaches are limited in their ability to understand and deal with systemic risks due to their necessary focus on single entities, systems and supply chains. As cybersecurity threats multiply, escalate and coalesce, it is imperative for the global community to treat cybersecurity risk as a systemic challenge that requires collective decision-making and coordinated action across governments, the private sector and civil society.

This briefing paper outlines how the technology and cybersecurity landscape is changing, why these changes make cybersecurity risk management a systemic issue, and how governments, international organizations, the private sector and civil society must collaborate to make society resilient to systemic cyber events.

1 The cybersecurity landscape

> What has changed is the capability and ambition of cyberthreat actors. Isolated cyberattacks can become major cyber events.

The World Economic Forum previously examined the issue of systemic cybersecurity risk in the 2016 *Understanding Systemic Cyber Risk* white paper. As predicted, societal reliance on technology has steadily increased since then as connected devices and cloud-enabled services have become more engrained into daily lives.

What has also changed is the capability and ambition of cybersecurity threat actors, as well as the availability of attack opportunities. Cybersecurity experts have feared that large-scale global cybersecurity attacks would materialize in the future. In the years since, this fear has shown itself to be well-founded:

- In 2017, a popular piece of Ukrainian accounting software was targeted to gain access to Ukrainian systems, referred to as the NotPetya attack. The attack spread beyond Ukraine, crippling international shipping among several other sectors, and resulted in estimated costs of $10 billion in total damages.
- In 2020, SolarWinds's IT management and monitoring platform software was compromised, and attackers had the potential to gain access to tens of thousands of organizations.
- In 2021, a piece of open-source logging software, Log4j, commonly used by apps and services across the internet, was exploited to potentially compromise hundreds of millions of systems.
- In April 2022, an attack by the ransomware gang known as Conti showed it could cripple Costa Rica's ability to collect taxes, issue payments, buy and sell goods, and even provide electricity.

While each event's technical details are different, they also share key characteristics. Isolated cybersecurity attacks can become major cybersecurity events, which are characterized by cascading effects across communities, economies and governments.

These sometimes have catastrophic consequences, such as the NotPetya attack, which could threaten global critical infrastructure. Although emerging technologies are creating new opportunities for economic prosperity, they are also giving rise to new and highly complex risks. These challenges are too big and too complex for any one organization to tackle.

2 Understanding systemic cybersecurity risk

Systemic risk refers to the possibility that a single event or development may trigger widespread failures and negative impacts spanning multiple organizations, sectors, or nations. Systemic risk is described in the Forum's 2021 report *Beneath the Surface: Technology Driven Systemic Risks and the Continued Need for Innovation* as a network of seemingly isolated risks that grow and spread across heavily interconnected and deeply ingrained products, services and systems.

In cybersecurity, technological and comparative advantages can incentivize different organizations, often from different sectors, to rely on the same third-party hardware, software, or service provider. For example, many firms might have a reliance on poorly maintained open-source projects, or on the same cloud company or Domain Name Services (DNS) provider. This concentrates risk when a shared service or commonly used technology is disrupted by cyberattackers.

This means that disruptions to organizations that do not appear to have a systemically important role in the digital ecosystem can have unexpected consequences.

Preparation for systemic cyber events requires collaboration across the private sector, government agencies and civil society. For this to be effective, there needs to be a common understanding of the risks that organizations are trying to identify and manage.

3 Classifying systemic cybersecurity risk

> Technological advantages can incentivize different organizations to rely on the same third-party hardware, software, or service providers.

Systemic cybersecurity risks can be broadly categorized by the source from which they originate and the way they manifest or present themselves within a broader system. While risks can manifest in a multitude of ways, they are likely to originate from one of the following source categories:

- **Common cause risks** include those risks that originate when multiple organizations utilize the same hardware, software, or communication tools, which create the possibility that multiple failures may arise from a single underlying defect.
- **Shared service risks** refer to the risks generated by organizations that leverage the same cloud providers or social media platform, for exampleto accelerate business operations, yet leave themselves vulnerable to cybersecurity incidents that the host provider could not anticipate.
- **Operational dependency risks** occur when the disruption in one organization's operations, such as a shut down of an electricity grid, disrupts many other organizations' operations, creating a cascading effect across multiple entities.
- **Shared trust and confidence** risks stem from activities with over-reliance on – and subsequent loss of – the trust that data and processes are accurate and reliable.

Systemic cybersecurity risks can manifest in a multitude of ways and can provide another angle through which risk could be understood.

- **Flow risks** include the risks that flow from one organization to another through a multitude of connection and interlinkages. This includes risks that transfer along physical or operational connections between organizations (sometimes described separately as chain risks).
- **Simultaneous emergence risks** are those risks that appear simultaneously across many different organizations.
- **Behaviour risks** are the risks propagated by many people or organizations changing their behaviour in a short period of time, such as when the COVID-19 pandemic caused many people to work from home.

4 Responding to systemic cybersecurity risk

Historically, the rate of technological innovation has outpaced regulation and policy actions, and cybersecurity threat actors have continued to rapidly learn and evolve. Effectively managing systemic cybersecurity risk at the speed and scale required cannot be left solely to individual governments or organizations, who are only part of the chain through which the impacts of a systemic cyber event are felt. Instead, a whole of global society approach is required.

Stakeholders across governments, international organizations, the private sector and nonprofits should identify the actions within their control and coordinate across different organizations to collectively address these problems.

Government policymakers

National governments can use their legal, regulatory and financial capabilities to incentivize country-wide efforts to study, respond to and manage systemic cybersecurity risks. Even though systemic cybersecurity risks often cross-national borders, countries can still take steps to understand the risks and lessen their vulnerability. Governments can:

- Continue to coordinate attribution and legal efforts to name, shame, sanction and arrest threat actors in order to deter future large-scale cybersecurity attacks
- Commission country-wide systemic cybersecurity risk research to quantify and track country-level cybersecurity risk and high-impact sectors
- Shift from event-based, responsive cybersecurity policies to proactive measures that address cybersecurity risks as part of a larger, interconnected system
- Continue to encourage and fund development security and operations (DevSecOps) transitions across government agencies
- Establish explicit cybersecurity requirements for the standardization of development of hardware, software and services that are provided to government agencies
- Provide financial backstops for cybersecurity insurance markets to incentivize cybersecurity insurance coverage and allow for coverage of certain systemic cyber events that are too big for the private insurance industry to bear alone
- Coordinate to identify, prosecute and deter large-scale criminal activity that targets critical infrastructure
- Facilitate information sharing within the national economy and engage with others on an international level

International organizations

International organizations can use their existing platforms and decision-making processes to develop new standards, propose international agreements and facilitate inter-governmental dialogue and collective action. By centralizing and coordinating global action, they can better address systemic cybersecurity risks that cut across multiple regions and types of governments. International organizations can:

- Establish global norms that prohibit state or state-sponsored cybersecurity attacks against core open-source projects, common digital and other critical infrastructure
- Create confidence-building measures to reduce concerns over governments targeting key foundational elements of the internet
- Develop cybersecurity capacity funds to help build cybersecurity capabilities. This will support lower-capacity countries to strengthen their cybersecurity postures and recover from large-scale cybersecurity attacks
- Charter an international working group to study and measure systemic cybersecurity risks and identify common vulnerabilities and bottlenecks

Private sector leaders

> Incentivize talent and knowledge exchange efforts with governments, international organizations and nonprofits.

The private sector is a powerful resource for cybersecurity talent, quick decision-making and innovation. Private sector organizations can take steps to secure their operations, protect their customers against systemic cybersecurity risks, and share best practices and lessons learned. The private sector can:

- Use a cybersecurity risk taxonomy to identify an organization's unique risk posture and vulnerabilities beyond an organization's direct control
- Set clear risk appetite standards and take measures to reduce exposure to cybersecurity risks and limit exposing customers or other organizations to these risks
- Support efforts to secure and maintain core open-source infrastructure projects
- Create and maintain software bills of materials, which list the items that make up the components for software products and services
- Incentivize talent and knowledge exchange efforts with governments, international organizations and nonprofits to diffuse innovative solutions across the global cybersecurity community

Cybersecurity nonprofit leaders

Cybersecurity nonprofits play an important and often overlooked role in the global cybersecurity ecosystem. Nonprofits are often seen as neutral experts, which allows these organizations to bring together diverse voices, perspectives and resources. These organizations can use their expertise to create, aggregate and disseminate tools to educate and secure organizations and individuals against systemic cybersecurity risks. Nonprofits can:

- Integrate and amplify diverse voices and perspectives from across the global cybersecurity community
- Educate organizations and individuals on the characteristics and dangers of systemic cybersecurity risk
- Create, aggregate and sustain tools, frameworks and resources to help organizations of all sizes proactively address and respond to systemic cybersecurity risks

Acknowledgements

This briefing paper is based on conclusions from meetings of the World Economic Forum's Global Future Council on Cybersecurity in its 2021-2022 session.

Lead authors

Michael Daniel
President and Chief Executive Officer, Cyber Threat Alliance

Colin Soutar
Managing Director, Cyber Risk, Deloitte

Global Future Council on Cybersecurity Members

Louise Axon
Research Associate in Cybersecurity, University of Oxford

Christophe Blassiau
Senior Vice-President, Cybersecurity and Global Chief Information Security Officer, Schneider Electric

Maya Bundt
Director, Bâloise-Holding; Chair, Cyber Resilience Chapter, Swiss Risk Association

Gabi Dreo Rodosek
Professor; Founding Director, Research Institute CODE, Universität der Bundeswehr München

Cathy Foley
Chief Scientist, Government of Australia

David Koh
Commissioner of Cyber Security and Chief Executive, Cyber Security Agency of Singapore

Renju Varghese
Fellow and Chief Architect, HCL Technologies

Global Future Council on Cybersecurity Manager

Seán Doyle
Lead, Centre for Cybersecurity, World Economic Forum

With support from:

Anthony Fratta
Specialist Leader, Cyber & Strategic Risk, Deloitte

Christopher W. Smith
Manager, Cyber & Strategic Risk, Deloitte

Mackenzie Mandile
Senior Consultant, Cyber & Strategic Risk, Deloitte

Drew Herrick
Senior Consultant, Cyber & Strategic Risk, Deloitte

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

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

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

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

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