WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Understanding Systemic Cyber Risk

Global Agenda Council on Risk & Resilience

October 2016

Contents

3 **Preface**

4 **Foreword**

5 **1. The Evolving Nature of Global Systemic Cybersecurity Risk**

- 5 What is systemic cyber risk?
- 6 Changing environment
- 7 Threat and attack evolution
- 8 Complex, unpredictable and cascading consequences

9 **2. Systemic Cyber Risk to the Financial Services, Transportation and Healthcare Sectors**

- 9 A. Financial services sector
- 10 B. Transportation sector
- 12 C. Healthcare sector

14 **3. Managing Systemic Cyber Risk**

16 **Conclusion**

17 **Endnotes**

19 **Acknowledgements**

REF 181016

Preface

Worldwide, people are starting to feel the effects of the dawning Fourth Industrial Revolution, a convergence of technologies that is blurring the lines between the physical, digital and biological worlds in ways that will profoundly affect people and economies around the world.

As digital technology innovations, such as the sharing economy, blockchain or the Internet of Things, are multiplying at an unprecedented pace and connecting more deeply with the physical world, cyber risks are likely to rise. The number of connected devices will almost triple by 2020, from 13.4 billion to 38.5 billion, and the proportion of products sold via e-commerce is expected to more than double – from 6% in 2014 to 12.8% by 2019. Indeed, *The Global Risks Report 2016* identifies cyber risks as among the most likely and most impactful risks, and calls for building resilience as these risks become increasingly tangible.

Global risks can only be effectively dealt with if there is a common understanding of their importance and interconnected nature, and a readiness to engage in multistakeholder dialogue and action. Against this backdrop, the Global Agenda Council on Risk & Resilience aimed to foster collaboration between the public and private sectors and academia to strengthen joint risk management frameworks that empower communities to build their own resilience to a range of risks, from environmental to financial.

Over the past two years (2014-2016) the Global Agenda Council published a series of publications, which aim at raising awareness and providing practical examples to inspire entities to build resilience to different risks through multistakeholder collaboration. These use cases deal with building resilience to epidemics and creating public-private partnerships in the face of natural disasters. In this White Paper, the use case, *Understanding Systemic Cyber Risk*, is the fourth publication in this series.

As the Council term draws to an end, gratitude is extended to Kirstjen Nielsen for her leadership as Chair of the Global Agenda Council, as well as to Council members Lauren Alexander Augustine, Stanley M. Bergman, Michael Berkowitz, Edwin Macharia, Victor Meyer, Paul Nicholas, Satoru Nishikawa, Yuichi Ono, Sara Pantuliano, Joe Ruiz, Armen Sarkissian, Dan Smith, Elizabeth Hausler Strand, Jaan Tallinn, Michael Useem, Margareta Wahlström, Nick Wildgoose and Alexander Wolfson for their contributions. Caroline Galvan managed the Global Agenda Council on behalf of the World Economic Forum.

For their dedication and contributions to this use case, special thanks go to Victor Meyer, Kirstjen Nielsen, Paul Nicholas and Nick Wildgoose. At the World Economic Forum, Derek O'Halloran advised on the content development and Stephanie Verin ensured report production.

Margareta Drzeniek Hanouz
Head of Global Competitiveness and Risks
and Member of the Executive Committee
World Economic Forum

Foreword

For over a decade, the World Economic Forum's *Global Risks Report* series has shed light on the increasing interconnectedness of our societies and the resulting evolution of the risks humans face. *The Global Risks Report 2016* (GRR 2016)[1] recognizes that these risks are becoming increasingly tangible, and identifies the "resilience imperative" – an urgent need to find new avenues to withstand, mitigate, adapt to and build resilience against global risks, predominately through deeper collaboration among stakeholders.

To encourage this process, over the past two years the Global Agenda Council on Risk & Resilience embarked on developing a series of resilience use cases, which sought to: 1) deepen the understanding of the global risk environment; 2) identify potential steps that entities could take to increase their resilience; and 3) distil the attributes needed for successful collaboration, based on individual stakeholders' capabilities, capacities and roles. The Council built on *Managing the Risk and Impact of Future Epidemics*[2] by developing reports on *Building Resilience in Nepal through Public-Private Partnerships*[3] and *Resilience Insights*[4]. The latter was developed to serve as a companion document to the GRR 2016 by proposing measures to address three of the risks identified. Completing this cycle, this use case – Understanding Systemic Cyber Risk – seeks to understand the nature and scope of emerging systemic cyber risk with examples from the financial services, transportation and healthcare sectors.

The *Global Risks Report 2016* finds that the risk of "large-scale cyberattacks" continues to be considered a high impact/high likelihood risk. Remarkably, however, the GRR 2016 also indicates that the evolving nature of cyber risk – from seemingly isolated attacks against specific companies (e.g. data breaches) to system-wide attacks with the potential for massive cascading effects (e.g. as recently occurred in the Ukraine energy sector) – is not yet fully understood as demonstrated by how experts perceive two risks closely related to "large-scale cyberattacks" (as identified and associated in the GRR 2016). Despite clear evidence of the growing internet connectivity of critical infrastructure services (including critical information infrastructure), the risk of "failure/shortfall of critical infrastructure" is perceived to be the sixth least likely risk with the second smallest potential impact, and the "breakdown of critical information infrastructure and networks" has continued to decrease in perceived impact over the last few years, and is considered among the least likely global risks to occur.

In fact, the GRR 2016 warns of the failure to understand risks related to technology as more organizations digitize their unique business value within increasingly connected environments that rely on machine learning and automated decision-making. Risks related to technology and cyberattacks might go unnoticed until it is too late, as organizations fail to account for their increasingly connected environments.

Today, every company is a software company.[5] Some forward-looking companies recognize the digital transformation and actively seek to build capabilities to respond to the hyperconnected environment. For example, Goldman Sachs "has more engineers and programmers working on tech matters than Facebook".[6] But today the vast majority of entities have yet to actually or fully recognize this transformation and as a result these enterprises can unknowingly assume tremendous risk. This risk may well exceed their individual capability for risk acceptance, mitigation or transference. Individually and collectively, this contributes to the likelihood of a systemic cyber event in one or more markets nationally and globally.

This use case goes beyond assessments of cybercrime and data breaches and begins to examine the emerging systemic nature of cyber risk that threatens to compromise, degrade or, in some instances, destroy key functions and capabilities. Two workshops were held to assess the nature of systemic cyber risk, and dozens of interviews and discussions were conducted with recognized global experts, owners, operators and senior private- and public-sector leaders. One finding was consistent – the meaning and implications of systemic cyber risk are not yet fully recognized or understood.

Section 1 of this paper therefore proposes some characteristics and a definition of "systemic cyber risk" to create a baseline for the discussion, and examines the environment operated in today. It ends with a discussion of how the changing environment and threat result in new and novel vulnerabilities with systemic cyber risk resulting in the potential for complex and cascading consequences. Section 2 then examines cyber risk to systems, assets and networks in the financial services, transportation and healthcare sectors. Section 3 identifies areas where additional thinking and analysis are needed and suggests some entities and actors who may be best positioned to lead the needed multistakeholder efforts. Through this use case, as with *Resilience Insights*, the intention of the Global Agenda Council on Risk & Resilience is to ignite an in-depth discussion about today's risks and to point the way towards building and strengthening resilience to address them.

1. The Evolving Nature of Global Systemic Cybersecurity Risk

A common lexicon to describe systemic cyber risk is currently lacking, and the understanding of the indicators, triggers or consequences of systemic cyber events is nascent. Therefore, to create a baseline for the discussion in this paper, a definition of "systemic cyber risk" is offered and the environment it operates in is examined. Hyperconnectivity, increasing digitization, the explosion of the Internet of Things (IoT), the expanding usage and availability of cloud services, and the pace of innovation, technology development and adaption all contribute to a quickly evolving environment. A brief overview of the evolution of the threat, threat actors and cyberattacks follows. This section ends with a discussion of how the potential consequences emanating from systemic cyber risk can be complex, unpredictable and cascading in nature; they will affect multiple entities, industries and geographic regions through contagion effects.

What is systemic cyber risk?

While significant efforts have been undertaken to study systemic risk, the International Monetary Fund (IMF) observed that "'Systemic risk' is a term that is widely used, but is difficult to define and quantify. Indeed, it is often viewed as a phenomenon that is there 'when we see it'."[7] The notion that "we will know it when we see it" is a very uncomfortable position for chief executive officers (CEOs), government leaders and more operational professional risk management experts in enterprises and regulatory agencies across all sectors of the global economy. Noting the lack of common lexicon to describe these concepts and the general nascence of current understanding, this paper seeks to begin to identify and define "systemic cyber risk".

Systemic risk is inherently different from non-systemic risk in that the consequences are more widespread – systemic risk is the risk of "breakdowns in an entire system, as opposed to breakdowns in individual parts and components"[8] – and more complex as multiple variables, connections, dependencies and interdependencies result in cascading, often unexpected, consequences. "Systemic risk events can be sudden and unexpected, or the likelihood of their occurrence can build up through time in the absence of appropriate policy [technology and/or management] responses."[9] In the latter case, modest tipping points can combine indirectly to produce large failures. For example, risk realized through common threat vectors across enterprises and ecosystems can result in large aggregate effects, especially where the "vulnerability" is integrated in operations common across enterprises. Systemic risk by its nature requires risk-sharing due to the risk of contagion, as one loss triggers a chain of others.[10]

Borrowing elements from the Group of Ten's 2001 definition of systemic financial risk, the following working definition and description are proposed as a starting point from which to begin exploring systemic cyber challenges across key sectors:

> Systemic cyber risk is the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security.
>
> The adverse real economic, safety and security effects from realized systemic risk are generally seen as arising from significant disruptions to the trust in or certainty about services and/or critical data (i.e. the integrity of data), the disruption of operations and, potentially, the incapacitation or destruction of physical assets.

As the IMF describes, two of the primary challenges related to understanding financial systemic risk are the lack of "modern examples" and the lack of transparency into highly integrated operations and the attendant interdependencies.[11] Similarly, no "cyber pandemic", widespread large-scale simultaneous cyberattacks, or targeted and successful attack on key underlying infrastructure on which multiple essential services are dependent have yet been witnessed that might be said to fall within the scope of the definition above. However, the lack of an example does not preclude the possibility of such an event. In fact, today's quickly evolving environment and the evolution of the threat, as further discussed in the subsections that follow, combine to increase the probability of such an event occurring.

Box 1: Position, Navigation and Timing Systems as Potential Single Points of Failure

In an ever more connected world where speed and accuracy are key, reliance on high integrity, precise positional, navigational and timing (PNT) data is growing. The applications of global navigation satellite systems (GNSS) services and data are expanding exponentially. The proliferation of these applications is delivering innovative capabilities that are allowing for increased accuracy and efficiency across business and industry – including in sectors such as financial services (e.g. settlement systems), transportation (e.g. ship navigation) and health (e.g. drug

manufacture and supply chain). In some cases, PNT is built into integrated systems/operations where its use and/or dependence on it is not recognized by those who use and depend on the system. In fact, many different systems already have GNSS as a shared dependency, so a failure of a PNT signal could cause the simultaneous failure of many services that are likely otherwise assumed to be independent of each other.*

Real-world disruptions of PNT data have shown that unexpected consequences occur from these disruptions, including in precision timing and positioning/navigation. PNT data can also be denied and manipulated, exposing operators to poorly understood threat vectors. To prevent degradations from disruptions of PNT data, system operators should understand when they are using PNT data and the precision of their PNT requirements. They should know the source of the PNT and have a backup secondary source that doesn't rely on the primary source (i.e. many backup systems are ultimately dependent on GPS), and they should also understand the ability of their systems to operate in a PNT-disrupted environment.

* The Royal Academy of Engineering, *Global Navigation Space Systems: reliance and vulnerabilities*, March 2011, available at http://www.raeng.org.uk/publications/reports/global-navigation-space-systems.

Isolated examples of denials of service (e.g. entity targeted ransomware) and data breaches (e.g. Target, Talk-Talk, etc.) – even if large and extremely costly – are not examples of systemic cyber risk. In fact, the overwhelming focus on data breach and credit-card hacks today distracts security experts, CEOs and government officials from the more fundamental and pernicious risks that could potentially trigger a systemic cyber event.

The blind spot of systemic cyber risk enables the aggregation of substantial risk that corporate boards cannot see, manage or mitigate. This creates an environmental condition across the global marketplace that, when hit with the right trigger or shock, could result in a wide range of unexpected and cascading consequences (over time and without geographical boundaries), including disruptions to the integrity of data and to operations, and even the incapacitation or destruction of physical assets.

The blind spot exists today in part because cyber risk assessments tend to be conducted in isolation and are often confidential, and because digital interdependencies, aggregated dependencies and single points of failure are not yet well understood and/or are not yet identified. As a result, entity-level risk assessments do not enable individual enterprise owners to gain a clear systemic risk picture that includes the risk to all entities, systems and networks to which they are connected. Even when there is clear agreement on shared interdependencies, such as payment and settlement systems and certain key energy generation transmission points, and on aggregated dependencies, such as air traffic control or position, navigation and timing systems (see Box 1), the opportunities are few for key market players in various sectors to fully understand more than the rudimentary attendant risks.

Systemic cyber risks can result from dependence on complex infrastructure undergirding essential functions but can also result from disruptions or loss of the confidentiality, integrity and availability of critical information (see Box 2).

Box 2: The Systemic Nature of Risk to the Confidentiality, Integrity and Availability of Critical Information

While much has been said about cyberattacks involving data breaches or theft, including from sensitive systems, a far more disconcerting scenario involves the alteration of critical data. If a rogue nation or terrorist organization had the capability to cause widespread disruption of essential services or damage to data integrity, organizations (private and public alike) may have difficulty containing the event. Unlike data breaches and extortion demands (e.g. through ransomware attacks), which inflict relatively small and targeted wounds, this kind of failure could have widespread ramifications. Such an attack is not only difficult to detect, but it also may be difficult to discern when the data were changed, thus making it difficult to "roll back" to a known good state and maintain business continuity.

For example, the loss of data integrity, the disruption of critical operations or the damage of certain physical assets could:

- Disable a key market play and indirectly impact other market players that rely on their key functions
- Spark a contagious disruption that could cascade and directly impact other market players and the broader economy
- Erode trust in key systems and services that are essential for the economy, defence or public safety

To begin a larger conversation around systemic cyber risk, this paper identifies some key vulnerabilities and potential single points of failure in the financial services, health and transportation sectors. The hope is that a deeper understanding of the potential consequences will help public and private entities refine their risk management strategies, identify new areas for investment, determine what partnerships need to be pursued, and generally build and strengthen their resilience.

Changing environment

Our environment is evolving at an unprecedented rate, reflecting the uptempo pace of innovation and technology. The growing digitization of systems, assets, data and networks, and rapid technological innovation are resulting in unprecedented efficiencies, new and increased capabilities and capacities, convenience, safety and security. In 2016, over 3.4 billion people are online, with the expectation that by 2025 more than 5 billion people will be online, an increase of 30% in just 10 years.[12] This massive growth in internet connectivity is only expected to accelerate, given the dramatic growth opportunities the online economy can offer individual entities, sectors and countries.[13] Research suggests that the effect of digitization and increased internet connectivity in emerging markets could be even greater and is therefore likely to result in an explosion of applications, services and devices.

The IoT, a natural evolution of the internet, is a key part of this new market economy. The number of IoT device types and uses is almost innumerable. According to a study conducted by McKinsey Global Institute, the IoT will have a total potential economic impact of between $3.9 trillion and $11.1 trillion by 2025.[14] As IoT deployments mature, its sensors and systems will enable data and decision-making that will dramatically improve operations and offer predictive – and even pre-emptive – maintenance for many services. IoT also enables real-time information that can contribute to operational resilience for many key operations, such as data related to the performance, status and condition of the devices.

Other technological advances, such as cloud computing, cognitive systems and big data analysis, also create efficiencies. Cloud computing and storage infrastructures or hyperscale cloud computing providers are rapidly expanding. Cloud computing not only offers flexible, elastic and economic solutions, but it also provides redundancy and geodiversity. As a result, cloud-based technologies can enable an entity to manage operations from many different locations during chronic stressors and in the inevitable event of acute shocks, therefore providing companies with a risk management platform.[15] IoT growth in particular will accelerate the adoption of cloud services and, by 2020, more than one-third of all digital information created annually will either live in or pass through the cloud.[16]

With significant growth in IoT and the cloud, machine learning and big data are becoming ever more important as a significant amount of previously untapped data are collected, assessed and digitized. These newly available data provide billions of dollars to potential businesses that can quickly and effectively evaluate the data.[17] Additionally, the International Data Corporation (IDC) forecasts global spending on cognitive systems[18] will reach nearly $31.3 billion in 2019.[19] IDC further sees cognitively-enabled solutions that "offer the tools and capabilities to extract and build knowledge bases and knowledge graphs from unstructured and semi-structured information as well as provide predictions, recommendations, and intelligent assistance through the use of machine learning, artificial intelligence, and deep learning".[20]

Conversely, as further discussed below (see "Complex, unpredictable and cascading consequences"), the aspects of connectivity, digitization, IoT, cloud services, big data analytics and cognitive systems that provide the opportunity for growth and efficiencies can also introduce new and novel threats and vulnerabilities simultaneously, increasing systemic risk complexity. For example, because IoT is the bridge between cyber and physical systems, a compromised IoT system could be much more destructive (see Box 3) than data loss or corruption, potentially resulting in physical harm to operations and humans. Also, small to medium-sized companies are able to leverage the inherent security that cloud services providers deliver as part of the solution. However, not all service providers are the same, and companies need to continue to assess the risk in this outsourced security model, as they are not able to outsource their accountability.

Box 3: The Evolution of Cyberattacks – Scale and Scope

Cyberattacks are evolving in terms of both scale – from isolated attacks against specific entities to industry-wide targeting, as was the case with the coordinated distributed denial of service (DDoS) attacks against the financial sector in 2012 – and scope, targeting systems that if penetrated could result in substantial cascading effects, as recently occurred in the attack on the Ukraine power grid.*

* See Corero Network Security, "New SEC Filings Show Impact of DDoS Campaign on Banks", April 2013, available at https://www.corero.com/blog/414-new-sec-filings-show-impact-of-ddos-campaign-on-banks.html; and Electricity Information Sharing and Analysis Center (E-ISAC), "Analysis of the Cyber Attack on the Ukrainian Power Grid", March 2016, available at http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

Threat and attack evolution

Reflected by newspaper headlines worldwide, the reported numbers and scope of cyberattacks continue to increase, and the techniques used to gain access evolve at the same pace as the defences raised to stop them. Innovation and inventiveness pay dividends for malicious actors, as do the neglect of basic security practices[21] and the lack of risk understanding. Reporters and security experts have made it clear that even though many organizations have invested substantially in cybersecurity, a well-resourced and persistent attacker can often be successful in reaching the desired targets.

Cyber threats remain difficult to assess despite over a decade of effort to understand and craft appropriate responses to them. The threat actors vary (from hacktivists to cybercriminals, to disgruntled or nefarious insiders or saboteurs, to nation states) as do their motives (from criminal activity such as fraud, theft or the distribution of child pornography, to economic or military espionage, to cyberwarfare[22]), which as a result make it more difficult to predict and quantify the impacts and consequences of a potential attack.

Cyber exploits are becoming stealthier and more persistent. While recent research shows that the average length of time attackers spend undiscovered on a network has decreased, the number still exceeds six months.[23] Isolated hacks have morphed, such that a single intrusion or a network scan is often only a prelude to further exploitation, and information theft or a data breach can be a precursor to system disruption or function loss.

Today's threats have evolved beyond crime to threaten the vital critical infrastructure that supports the economy, national security and public safety. The attack on the Ukrainian power grid in 2015 demonstrated a significant escalation of the threat,[24] but was one of many examples where a cyberattack against an industrial control system can create physical consequences and result in billions of dollars of damage.[25] Again given current capabilities, one can identify a variety of possible motives – a systemic cyberattack could be an action to "prep the battlefield", an aggressive move to disable, slow down or remove large-scale competitors, or an action to demonstrate a show of force/deterrence.

Complex, unpredictable and cascading consequences

As referenced above, the gains in efficiency and capability derived from increased digitization bring new, complex and evolving risks. Today's multifaceted configurations provide ample targets for hackers to exploit. For example, each of the current 50 billion connected devices could offer a potential vulnerability to be exploited by hackers. Malicious actors could disrupt or manipulate the "dialogue" between device and controller, or seek a path into a larger network. The damage from a breach of the IoT may also go far beyond individual annoyance to having a widespread financial impact. Because it may involve the control of physical processes, "cyber as a peril" now includes property damage, bodily injury and, possibly, death.

The actual impact of a given disruption will depend on many factors and can be difficult to predict and quantify[26] – making it difficult to plan and allocate resources to meet the risk. The reaction of systems and institutions to a particular disruption may significantly influence whether and how a disruption spreads. These reactions may be very difficult for other parties to anticipate (due to blind spots, already mentioned).

Reliance on highly connected and interconnected technology gives rise to:

- The *creation of single points of failure* (e.g. SWIFT[27])
- *Sets of concentrated dependencies* (e.g. reliance on a diminishing number of large ports in the shipping industry;[28] or, as a large number of businesses have grown dependent on software or hardware solutions provided by a small number of outsourcing vendors, should there be any compromise in the confidentiality, integrity or availability of the data stored by those vendors, ramifications would not only be felt by the customers of those vendors, but also the end users of every business affected)
- *Complex interdependence* (e.g. relationships between supervisory control and data acquisition and operations, which depend on each other's data, operations and thresholds)

These vulnerabilities in turn can lead to cascading consequences if the cyber risk is realized. Such cascading consequences can propagate:

- Sequentially from one system to another: this potential effect arises when the smooth functioning of one or more systems is conditional on that of another system (e.g. an upstream example, cyber financial systems depending on the continuous availability of electricity)
- Simultaneously to many systems: this potential effect stems from many systems depending on other critical systems, or on key service providers (e.g. the financial services, transportation and healthcare sectors all depending on the uninterrupted functioning of position, navigation and timing systems)
- Beyond systems and their participants to other markets and sectors (e.g. a systemic failure of the financial services sector having catastrophic effects on economic and national security worldwide)

Section 2 explores concrete examples of systemic cyber risks and the potential associated consequences across the financial services, transportation and healthcare sectors. This paper examines cyber risk specifically and therefore narrowly focuses on the downstream consequences of a potential attack on institutions rather than the risks they face upstream – one such example would be the dependence on electrical supply for the entities in question.

In short, the changing nature of the threat, utter dependence on technology, and current blind spots on the scope of systemic risks should give CEOs and government officials pause for thought. The complexity of today's economic landscape and the reliance of key sectors of the economy on online services mean that the risk and probable consequences are not well understood and not easy to quantify. The ability of entities to prepare for the consequences of systemic risk and build common processes, capabilities and capacity to enhance their cyber resilience, and ensure they are able to recover from a systemic cyber event, is therefore more important than ever.

2. Systemic Cyber Risk to the Financial Services, Transportation and Healthcare Sectors

A. Financial services sector

Financial services sector overview
The financial services sector is highly diverse. According to the US government, it includes:

… thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions. Financial institutions vary widely in size and presence, ranging from some of the world's largest global companies with thousands of employees and many billions of dollars in assets, to community banks and credit unions with a small number of employees serving individual communities.[29]

Together these organizations are a vital component of the global economy, and the networks and systems that provide financial services form the backbone of global commerce. Recent decades have seen the volume and value of financial transactions increase tremendously, owing both to financial innovation and advances in information and communications technology (ICT). As a result, the importance, but also complexity, of certain financial services systems has grown exponentially. Some of the core functions of financial services are payments, market provisioning, investment management, insurance, deposit and lending, and capital raising.

Financial services represent one of the most connected components of the modern economy. Financial services entities are connected through networks of electronic systems with innumerable entry points. Financial systems are interconnected in a variety of ways. Tighter direct relationships between systems, stronger indirect relationships arising from the activities of large financial institutions in multiple systems, and broader commonalities, such as the use of common third-party service providers (e.g. SWIFT, RTGS), have led to a complex web of interconnections. As a result, the settlement flows, operational processes and even risk management procedures of many systems have become more interdependent and dependent on key providers.

For example, today, payment and settlement systems rely on messaging services to transmit transaction-related information, such as payer, payee and the amount to be transferred. Neither a payment nor a settlement system, SWIFT is one example of several systems underpinning global financial systems that connect into broader bank networks and are remotely accessible. Most financial institutions in the world have a SWIFT connection, which provides a critical global messaging platform to the financial sector and is designed to service more than 10,000 financial institutions in 212 different countries. Another example is gross settlement systems, such as real-time gross settlement systems (RTGS), which have been introduced by many countries to facilitate enhanced risk management for the handling of critical payments. Gross settlement systems such as RTGS help reduce the interbank credit exposures arising from a delay in settlement.

Systemic cyber risks to the financial services sector
While all financial transactions are exposed to a level and variety of risks, payment, clearing and settlement arrangements in particular are of fundamental importance for the functioning of the financial system and the conduct of transactions between economic agents in the wider economy. If modern economies are to function smoothly, economic agents must be able to conduct transactions securely and efficiently, and public trust in payment instruments and systems must exist if they are to effectively support transactions. Such trust could easily be shattered if the security and reliability of financial data are called into question, for instance through a cyberattack on the clearing and settlement systems (see Box 4).

In financial markets, market liquidity is critically dependent on confidence in the security and reliability of clearing and settlement arrangements for funds and financial instruments. If they are not managed and secured properly, the legal, financial and operational risks inherent in payment, clearing and settlement activities have the potential to cause major disruption in the financial system and the wider economy.

Box 4: 2016 Attack on SWIFT

Systemic cyber risk recently came under close scrutiny with the discovery of three separate hacking incidents against member institutions connected to the SWIFT network at banks in Bangladesh, Vietnam and Ecuador, which accounted for more than $90 million in stolen funds. While the attacks' main purpose appears to fall into the category of traditional cybercrime, the hacks demonstrate that the applications that enable the financial messaging traffic between member banks can be manipulated and misused when member institutions do not strictly adhere to the security standards.

Formerly, accessing the SWIFT network required being physically present at a dedicated terminal. However, as banking requirements and technologies have changed, the ability for financial institutions to connect to this network has changed as well. Banks now leverage multiple applications, resident on various user endpoints, to interface with the SWIFT network. Each connected endpoint presents an avenue of attack for threat actors to fraudulently create and send financial messages. The Bangladesh Central Bank

hack is a prime example of this situation; a crafty threat actor infiltrated a poorly-secured network and used an unsecured endpoint in an attempt to carry out one of the largest bank heists in history.

Any significant or prolonged disruption impacting payment, clearing and settlement arrangements could touch all major aspects of financial risk, such as:

- Credit risk – defaults on obligations within the payment system, imposing direct unexpected loss on other participants
- Liquidity risk – insufficient liquidity to fulfil settlement obligations
- Market risk and business risk – other transactional risks, including loss of revenue arising from suspension of payment services due to disruption or insolvency

While the potential patterns of attack on the financial services sector can vary significantly, they could include, but are not limited to:

- A number of simultaneous cyberattacks on systemically important institutions and critical/core financial infrastructures
- A large-sale cyberattack on the SWIFT network, potentially coming from a connected institution or directly impacting SWIFT, forcing SWIFT to discontinue the service or shutdown traffic
- A coordinated, simultaneous cyberattack on the RTGS or SWIFT network, resulting in a widespread disruption that could create short-term catastrophic results in a global economy
- A cyberattack on crossing systems or automated trading that could take advantage of trading complexity and capacity, increasing the risk of disorderly markets – through the malfunction of algorithmic programmes – and the risk of market misconduct, such as unsolicited information leakage and possible market manipulation of "dark pools" (private exchanges for trading securities).

Impact and consequences of systemic cyberattacks in the financial services sector

Closer connections have helped to strengthen the global payment and settlement infrastructure by reducing several sources of risk, and payment systems and related platforms are now less centralized and thus less susceptible to triggering a global shock in the case of an isolated disruption event. However, it is critical to acknowledge that the complex nature of these systems and processes makes it difficult to respond to and isolate issues in case of a coordinated cyberattack. Furthermore, tightening interdependencies have also increased the potential for disruptions to spread quickly and widely across multiple systems and markets. Both RTGS and SWIFT systems, because they are vital to cash and securities payments and settlements, are considered systemically important and potential "single points of failure" in the payment infrastructure globally. Given its complex connections, the consequences of an attack on "systemically important institutions" could quickly promulgate beyond systems and their participants to financial markets. For example, if the latter were not able to submit payment instructions, due to either operational or financial difficulties, the outcome could be widespread liquidity dislocations. The functioning of markets with relatively short settlement cycles, such as the markets for uncollateralized overnight loans and repurchase agreements, might be particularly affected. In the extreme, the inability of settlement banks to send payments raises the possibility of "liquidity sinks" developing in an RTGS system, as available liquidity becomes concentrated in the settlement account of the bank(s) concerned. Therefore, systemic cyber risk for the sector includes the potential for cyberattacks to result in:

- Failure of an institution's ability to meet its payment or settlement obligations, which could trigger a contagion effect where other financial institutions would not be able to meet their settlement obligations
- Failure or severe or prolonged disruption of a core payment and settlement system, which can be compromised at various endpoints, affecting multiple country and locations' securities markets
- The loss or compromise of the availability and integrity of key financial data
- Widespread loss of trust and confidence in the payment and settlement systems

In such a scenario, central banks may be forced to take exceptional measures, such as the injection of liquidity funds, repurchase agreements, guarantees to extend the settlement window, and reductions in the cost of intraday and overnight borrowing, among others.

Innovations in digital and communications technologies around the world have rapidly changed the landscape of payments and settlement systems. Ensuring the integrity, security, efficiency and continuity of these systems and networks in this dynamic environment will remain critical for the financial services sector and the world economy writ large.

B. Transportation sector

Transportation sector overview

The transportation sector includes the systems, networks, assets, people and vehicles of multiple transportation modes, including aviation, highway and motor carrier, maritime, mass transit and passenger rail, freight rail and shipping, and can also include pipeline systems. The transportation sector today is a truly global endeavour that plays a key role in the movement of people and goods, underpinning international trade and commerce. Global trade has been a key part of increased wealth creation over the last 20 years and it has tracked, in overall terms, at a higher rate than global GDP growth. Transportation systems also provide lifeline services to communities and are vital to response and recovery operations. With the population due to grow by another 2 billion by 2050,[30] mostly in cities, the need for efficiently operating transport infrastructure is only increasing. The latter – in turn – will need to rely on resilient, compliant and reliable data connections and infrastructures.

For many decades, transportation and logistics companies have invested much of their time and money into ensuring the integrity and reliability of their physical infrastructure and assets. Airlines and express operators have, for instance, been very mindful of the risks to their business stemming from a possible bomb on board an aircraft or in a shipping container. Physical screening of consignments and the

validation of shippers are commonplace. All major logistics companies also have huge security operations in place to prevent theft of shipments from their warehouses, the substitution of counterfeit goods or the use of their networks to move illegal drugs or firearms around the world. However, relatively less attention has been paid to the possibility of a cyberattack on their IT systems, which, depending on the source of the threat, could have consequences ranging from inconvenient to catastrophic.

The risk is very real: the Zurich/Business Continuity Institute *Supply Chain Resilience Report 2015*[31] lists IT problems and cyber risks as the top two causes of supply chain disruption. Also, large-scale data breaches – which could be precursors to disruptive events as attackers can use schematics or supply chain data to systemically disrupt trade and commerce – are common in the sector.[32] In line with these findings, the attitude across the industry is changing and can be summarized by one transport security expert who commented that while five years ago he was spending most of his time on the physical aspects of security, now the majority of his time is dedicated to technology and data exchange issues.

Systemic cyber risks in the transportation sector

Cyber threats to the Sector are of concern because of the growing reliance on cyber-based control, navigation, tracking, positioning, and communications systems, as well as the ease with which malicious actors can exploit cyber systems serving transportation.[33]

Much like the financial services and healthcare sectors discussed in this paper, the transportation sector is both very fragmented across its constituent components and dramatically interconnected. At the same time, the sector itself is increasingly reliant on information technology and data flows across navigation, propulsion, freight management and traffic control, irrespective of whether ground, water or air transportation and their associated supply chains are examined. With the development and deployment of e-freight or e-maritime systems, the risk is increasing along with operational efficiencies, as criminals, terrorists, security agencies and so-called hacktivists are increasingly targeting the information and communications technology systems relevant to transportation and logistics, whether for personal gain or economic or security disruption.

Importantly, the transportation sector underpins other aspects of the economy, and even the small selection of potential risks affecting the sector can demonstrate their systemic importance, or indeed highlight potential single points of failure. They include:

- Manipulation of data, or shutting down, of air traffic control systems, leading to immediate impact on the global travel industry
- Loss of trust in road transportation, following vehicular accidents resulting from hacks
- Tainted traffic control systems in smart cities, resulting in accidents, injury and death
- Distorted status of freight movement in trucks, trains, ships and aircraft, damaging goods and creating general supply chain turmoil

Given the highly interdependent nature of the sector, the transportation sector would also be severely affected by systemic failures that might occur in financial payment systems, which are required to ensure transportation systems continue to operate.

Box 5: Sector-Specific Attacks Case Study

While malware does not discriminate, it can be developed to target a particular industry. "Zombie Zero" malware represents just such an example and it underscores the growing cybersecurity risks faced by shippers and their logistics and transportation partners in a wireless, mobile world where technology changes rapidly.

Logistics firms use scanners to track shipments, as they are loaded and unloaded from ships, trucks and airplanes. Zombie Zero targeted the scanners at shipping and logistics firms for over a year. Once an infected scanner was connected to the target's wireless network, it attacked the corporate network and the scanned information, including origin, destination, contents and value, and shipper and recipient information was compromised.

The logistics industry also faces threats (see Box 5), but here the primary motivation is unlikely to be disruption of services, as for instance with the airline sector, but access to the goods themselves. The very shipment-level and supplier information that parties are encouraged (or required) to share with their suppliers and their customers is also invaluable to criminals and adversaries, who seek to disrupt logistics for political or economic gain, heightening the risk that the integrity or confidentiality of that shared information could be compromised. The widespread use of handheld devices and GPS technology in the field is increasing the risks. While companies have made strides to understand and manage this risk internally, they have difficulty identifying and managing it across a large supplier base.

Impact and consequences of systemic cyberattacks in the transportation sector

The interconnected nature of the transportation sector and its centrality to the efficient functioning of the global economy have meant that the actors in this sector are particularly at risk of systemic attacks that could have consequences that reach far beyond the entity immediately affected. It is clear that transportation systems are very interconnected and interdependent, and that the complex nature of these systems and processes makes it difficult to respond to and isolate issues in case of a coordinated cyberattack. These closer interdependencies have also created additional single points of failure and increased the potential for disruptions to spread quickly and widely across multiple transportation and supply chain networks.

While an impact of a single cyberattack on an entity within the transportation system is difficult to estimate, given not only the myriad of different methods and objectives the attackers could have, but also the sheer diversity of the sector, it is clear that if an attack were to breach critical systems on which communication nodes for the sector depend, consequences could be catastrophic. In the previous section, examples were given that illustrate the critical importance of the transportation sector to a particular subset of an economy. If such an attack were to take place in a key

logistic hub, the effect would be multiplied with the potential for disruptions to spread widely and quickly across transport, logistics and supply chain networks around the world. Such an attack, particularly if it resulted in a systemically important institution's inability to perform their logistical functions, could also quickly affect the normal functioning of supply chains and, as a result, could lead to widespread economic and humanitarian issues. In the extreme, for example, the inability of pharmaceutical supply chains to operate effectively will affect human life.

Examining the consequences of systemic cyberattacks in the aviation sector demonstrates the possibility for widespread and cascading consequences. Aircraft design is increasingly reliant on network connectivity and electronic data exchange for efficiency gains, making the industry ever more reliant on the transfer of real-time automated data from ground to aircraft. If the systems were compromised, consequences for the safety of the crew, passengers and cargo could be disastrous. The same can be said for air traffic control systems or position, navigation and timing systems. In fact, in June 2015, the Polish national airline, LOT, announced that it cancelled flights due to a cyberattack against the airline's ground computer systems at Warsaw's Okecie airport that left it unable to create flight plans.[34]

The consequences of a potential port closure due to a cyberattack are another example of the effects resulting from concentrated dependency or single point of failure. As shipping has become increasingly channelled through the ever-decreasing number of ports capable of loading and offloading the largest container ships, single points of failure exist in both physical and online worlds. For example, a successful cyberattack on a port community system (a system responsible for the coordination of all port activities) of one of the big "gateway" hubs, such as Rotterdam or Los Angeles, would have a substantial region-wide economic impact due to the lack of options available for the rerouting of ships.

Some of the consequences could include:
- Increased pressure on other ports and associated infrastructure to cope with redirected throughput
- Immediate cost and delays as a result of rerouted vessels
- Subsequent construction project delays
- Potential manufacturing holdups
- Delays or even the non-arrival of key food or health products
- Financial repercussions at the port and throughout the port's supply chain at the micro and macro levels

The possibility of systemic failures is significant because systems are operating within systems, such that the interconnected physical movement of goods must be synchronized appropriately with the associated necessary data flows.

C. Healthcare sector

Healthcare sector overview

Information is the lifeblood of healthcare. Interconnected systems provide for the delivery life cycle of healthcare-related services, including the assessment, diagnosis and treatment of patients (in pre-hospital medical practices to traditional hospital or specialized care settings); the development of new and novel approaches to cure diseases and establish treatment plans; the development, manufacture and delivery of medical devices and pharmaceuticals that are part of those plans; the availability of medicines and devices via pharmacies; and the overall management of health services and the administration of health insurance. Healthcare sector systems acquire, store and process a vast amount of critical and sensitive personally identifiable information (PII), such as bank account information, credit card data, social security numbers and electronic protected health information (ePHI), such as medical diagnoses, insurance claims and treatments, each step of the way.

The healthcare sector as a whole is increasingly reliant on ICT to leverage this wealth of information in order to provide a high level of care for patients, but different segments have found different uses for its capabilities. Hospitals and other healthcare groups collect and retain massive amounts of personal and confidential information about their patients, employees, procedures, research and financial status, largely to ease the use of doing business. On the other hand, pharmaceutical companies have embraced cloud computing to speed up their drug development processes, using technology to create actionable insights and to improve patient outcomes. And with the IoT, wearable, digestible and implantable technology is being developed and used to monitor and treat patients. As a result, worldwide healthcare data are expected to grow fiftyfold between 2012 and 2020.[35]

The opportunity benefits of the sharing and exchange of this information for continually improving the standards of care of patients also involve opportunity costs as attackers leverage this information for selfish reasons and by unlawful means. According to the US Department of Health and Human Services, 1,614 breaches of unsecured protected health information (PHI) have been reported since 2009, affecting nearly 160 million individuals.[36] Healthcare information and systems are under attack. The healthcare industry has become vulnerable to cybersecurity threats, whether from the growing use of big data for R&D in life sciences, reliance on cloud computing to improve the accuracy of assessments for insurance companies, increased reliance on technology to perform operations, the growing connectivity of medical devices, or the growth of healthcare-related information and electronic health records. In addition, the exponential growth of the systems for processing the large amounts of data that enable medical systems and services has far exceeded the pace of the required cybersecurity investment (as compared to other sectors) to ensure the cyber resiliency of these systems and the implementation of the requisite information protection capabilities.

The resulting low barrier to (illegal) entry, combined with the lure of lucrative healthcare data (and easy access to credit card information, which is frequently retained on the same systems), has made this sector one of the most targeted industries in recent years.[37] The concentration of personal information contained in electronic health records is extremely profitable for cybercrime actors.[38] In addition to using the personal information for direct financial gains (i.e. credit card and other financial fraud), attackers attempt to obtain illegal drugs and/or medical equipment and supplies, or participate

in healthcare fraud. And the threats are only increasing: 2016 has seen a proliferation of sophisticated malware attacks and social engineering campaigns for the sector, in addition to an upsurge of distributed denial of service attacks and extortion attempts through targeted ransomware campaigns on vulnerable healthcare institutions.

Systemic cyber risks in the healthcare sector

Similar to the transportation and financial industries, the healthcare sector faces a range of risks stemming from its production of critical information and reliance on key infrastructure. The targets are many. Cybercriminals can focus efforts not only on patients, but on healthcare providers, insurers, pharmaceutical manufacturers and distributors as well. Cybercriminals can use multiple methods of entry, such as phishing, stealing laptops, capitalizing off human error, social engineering and more.

While an increasing number of data breaches, ransomware attacks and individual cyber-related events have been reported by various healthcare-related entities with respect to financially motivated data theft, how do these threats and vulnerabilities translate into systemic risks to healthcare?

The healthcare sector's lack of comparative investment in cybersecurity has resulted in a widespread dearth of foundational security best practices to ensure the confidentiality, integrity and availability of critical and sensitive personal and health-related information. Confidentiality has been breached with the hacking and exfiltration of data for financial gain, both traditional theft and attacks, such as a ransomware attack, seeking to extort and/or blackmail through the threat of revealing sensitive PII and/or ePHI details. This uncovers significant gaps in cybersecurity resiliency related to critical healthcare information and systems.

The integrity of medical records can be put into question, potentially resulting in incorrect diagnosis and/or treatment with severe, possibly deadly, consequences to the patient. For example, nefarious attackers could change the blood type of a patient, and attackers leveraging stolen healthcare information can get access to controlled substances, the access of which becomes part of the stolen record. As the many parts of the healthcare life cycle are interconnected, incorrect and/or unavailable patient records could inhibit or alter potentially life-saving emergency medical care, as a patient moves through the system of care. Also, the process of manufacturing, testing and distributing potentially life-saving drugs can be disrupted due to a lack of integrity in the common supply chain sources, inaccurate clinical trial data from clinical research organizations and critical infrastructure transportation service issues. Here, the systemic nature is one of scale. For example, if the integrity or availability of large portions of the population's health records were called into question, the situation could completely disable a collective response to a pandemic situation, where the ability to deliver a response globally would be inhibited by a lack of availability of needed health information.

Attacks on these inherent healthcare system vulnerabilities can emanate from anywhere in the world and can have a profound impact on how routine and emergency care is provided to patients. It could extend the bad guys' motives from cybercrime to destructive attacks, and pose a threat to the delivery of effective healthcare services globally.

Impact and consequences of systemic cyberattacks in the healthcare sector

As indicated throughout this section, the healthcare sector is under siege by cyberattacks (also see Box 6), largely driven by the promise of easy riches for cybercriminals, but with the clear potential to expand to other causes and motivations. Moreover, the sector's response process can be slow, with individuals being informed of a potential disclosure up to a year after the breach has been found. Ultimately, this continued criminal exploitation could lead to the long-term degradation of trust in the use of ICT for healthcare. The damage to R&D in particular, which in recent years has relied on new technologies to accelerate the development of new drugs and deepen the understanding of human bodies to an unprecedented level, would be irreparable. Furthermore, the loss of trust in online healthcare delivery systems could dramatically impact remote communities, emerging markets and the response to urgent medical events, such as natural disasters and epidemics.

The healthcare sector could potentially however be exposed to more than just cybercriminals.

Box 6: Medjacking the Hospira Infusion Pump Case Study

Cyberattacks targeting healthcare monitoring devices (Medjacking) emerged in 2015. Security researchers discovered security flaws in the Hospira infusion pump that could remotely force multiple pumps to dose patients with potentially lethal amounts of drugs. In addition to insulin pumps, deadly vulnerabilities were found in dozens of devices, including X-ray systems, CT scanners, medical refrigerators and implantable defibrillators. After the researchers' discovery, the US Department of Homeland Security and Federal Drug Administration began warning customers not to use the devices due to the vulnerability. The announcement was the first time the government advised healthcare providers to discontinue the use of the medical device.

The real threats come from the possibility of terrorists groups, or even nation states, manipulating the technology not to access information, but to effectively put lives in danger. While such attacks have not yet publicly materialized, the danger is very real and could include:

- Widespread disruption of network-enabled medical devices like pacemakers or medicine delivery systems
- Widespread tampering of personal medical information, which could result in patients not receiving needed medications or incorrect dosages resulting in illness or death
- Altering of environmental controls in patient care facilities, causing patient distress or spoilage of medicines
- Network disruptions resulting in the unavailability of patient data and history during crucial moments and large-scale medical responses (such as in a pandemic)

3. Managing Systemic Cyber Risk

Given the complexity of the systemic cyber risk environment – the cyber risk footprint of any given entity is no longer limited to the entity's owned or controlled systems, networks and assets – it is not possible for any entity to address its cyber risk in a vacuum. A person's cyber risk includes another person's cyber risk if they are virtually connected, and the aggregated risk becomes the risk to individual systems and networks. Nor, as previously described, does any given entity have all of the authorities, capabilities and capacities to effectively address the scope of the risk or the pace of its evolution. Finally, given the sophistication and persistence of the threat, it is no longer enough to design a risk management approach towards "if we are attacked". Rather, risk managers must change their perspective to "when we are attacked" and "how often" and "how long can we resist an attack".

Unfortunately, while it is natural to want to stop an attack and understand the vulnerability, fix it and resume operations, centring on specific cyberattacks, events, incidents and campaigns, which places the focus on the attackers and their specific targets, may not be enough. Today the scope, scale and character of our dependence on cybertechnologies and systems are profound and increasing. The digital transformation of the modern enterprise should prompt CEOs and boards to reset their risk management assumptions. Similarly, governments and regulators need to re-evaluate their assumptions regarding the implications of these changes to our economic stability and security. They are inherently positive. But they are not without risk.

Traditional models of risk calculation seem to fall apart when it comes to assessing cyber risk, and it is an understatement to say that government and industry are struggling to understand and to prepare for the magnitude of systemic cyber risk. As already described, in part this is because a systemic cyber event or crisis has not yet been experienced. To some degree, systemic cyber risk is a bit of a "black swan". Black swan events: 1) are a surprise; 2) have a major impact; and 3) are retroactively predictable.[39] In other words, if a systemic cyber event occurs, the world will likely express shock at our dependence on technology, be stunned by the breadth of the impact and then essentially say, "Of course we knew that was going to happen someday."

But it is not necessary to wait until it happens. Action is possible now. To understand and manage systemic cyber risk, organizations must partner with suppliers (and suppliers' suppliers), customers and other virtually connected entities to understand the potential scope, scenarios and triggers for systemic cyber events. It is necessary to identify and assess together the critical infrastructure assets at risk, the vulnerabilities that may expose those assets and the capabilities and motives of the threat actors targeting those assets.

Identifying and understanding systemic cyber risk is only the first step; entities of all sizes, public and private must work collectively in partnership using all the capabilities and capacities at our mutual disposal to address it. Towards that end, it is important to recognize that many traditional approaches to risk management and governance that worked in the past may not be comprehensive or agile enough to address the rapid changes in the threat environment and the pace of technology change that is redefining public and private enterprises. Traditional cyber response or cyber defence tools, such as firewalls or automated threat indicator sharing, are no longer sufficient when facing systemic cyber risk. Furthermore, many common defences have been designed to limit the immediate impact to a particular individual or company, often with the main objective of protecting financial information or limiting financial impact. They have not been designed with persistent attackers with the resources of nation states in mind, nor to address risks that exist outside the realm of a given entity's control. Entities must be able to operate in the face of advanced persistent threats and attacks and to adapt to changing vulnerabilities and pressures. In partnership, a cultural, multistakeholder approach must be created and sustained - one we call an Advanced Persistent Resilience (APR) approach.

This analysis demonstrates that a more holistic approach to resilience is required, given the complexity of the cyber risk environment and the unique nature of systemic cyber risk. The APR approach combines the best of current operations, training, technologies and management processes and governance to enable entities to adopt, innovate, respond and mitigate – while under consistent attack. Contrary to a static compliance regime, the APR approach requires constant monitoring of the threat, and adjusting to and anticipating it. Risk managers must not only examine technical controls, but also the organizational culture, training, the comparative performance within peer groups and corporate governance.

Recommendations to Better Understand and Manage Systemic Cyber Risk

– World Economic Forum: The Forum can envisage convening a high-level group of experts and global thought leaders to explore the concept of systemic cyber risk and: 1) determine and capture the depth of understanding that currently exists in the marketplace around systemic cyber risk; 2) propose a definition of systemic cyber risk as an agreed upon lexicon is sorely missing in this area; 3) assess the potential scope of liability that enterprises are unknowingly assuming (including tail risks); 4) assess the economic and security implications to the global economy or key sectors of the potential consequences (including cascading consequences) resulting from a realized systemic risk in key sectors; and 5) create tools to help C-level executives and boards ask the right questions to both understand the risk and address it.

  The Forum can also investigate launching an effort to understand the culture and leadership dimensions of resilience. This effort should explore how leaders can motivate teams to explore new ways of analysing risk and methods for encouraging groups to develop the key attributes and capabilities for resilience in partnership, recognizing today's interconnected risks. Cross-sectoral, interdisciplinary and geographically diverse experts could be convened to further articulate the APR risk management approach and concept.

– The Organisation for Economic Co-operation and Development (OECD): The OECD should undertake an effort to study the current understanding of systemic cyber risks, explore possible systemic cyber events, and work with governments, the private sector and academic experts to identify potential indicators, metrics and triggers to include aggregated dependencies, single points of failure and tightly coupled cyber interdependencies. The establishment, integration and ongoing maintenance of metrics are vital to enable a shared understanding of the risk.

– Insurance and the modelling industry: A renewed focus should be given to the development of holistic interdependency models and the identification and assessment of cascading consequences within and among industry sectors and geographic regions. Specifically, systemic cyber risk quantification models that consider and include the tail risk of multiple cascading consequences are needed. These models can help not only to drive a further understanding of the accumulated financial exposures but also to support the process to integrate the appropriate risk costs.

– Governments: As the threat expands beyond industrial espionage to activities that trigger national security (e.g. the disruption of critical infrastructure services through cyberattacks), governments should work with the private sector to further articulate roles and responsibilities. Governments should transparently and inclusively develop incident management plans with private-sector entities to address large-scale cyber events. Understanding how the government will respond during a national cyber incident will enable the private sector to tailor its expectations and to plug into the larger effort as appropriate.

Governments must also clarify the "owner" of various types of risk and develop incentives to enable the least cost avoiders to take needed action to prevent or mitigate attacks.

– Cross-industry: The tightly integrated economic sectors, such as the financial services, transportation and healthcare industries, should convene vertical working groups of experts in insurance, technology and operations to explore the key dependencies common to enterprises and the processes and functions on which the whole sector relies.

Conclusion

Cyberdependency and the dramatic technological transformations that are happening to enterprises, infrastructures and systems globally are profoundly resetting the traditional expectations of risk management and its approaches. Systemic cyber risk presents a fundamentally new challenge. Investment in understanding it is needed before a systemic cyber event occurs. Otherwise, the cost will be far too high. Seeking to partner, analyse, test and investigate the range of triggers and the scale of consequences that could result from such an event is essential. In parallel, seeking to develop and grow a new generation of preparedness and readiness based on an APR approach is also necessary.

No ready-made curricula on systemic cyber risks and how to best manage them exist. This paper offers the beginning of a dialogue that will hopefully span both public- and private-sector organizations. Much can be debated and discovered with respect to systemic risk and resilience and the appropriate roles and responsibilities of the various players in the ecosystem to combat the risk and build resilience.

Endnotes

[1] World Economic Forum, *The Global Risks Report 2016*, 11th Edition, available at http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf.

[2] World Economic Forum, *Managing the Risk and Impact of Future Epidemics: Options for Public-Private Cooperation*, June 2015, available at http://www3.weforum.org/docs/WEF_Managing_Risk_Epidemics_report_2015.pdf.

[3] World Economic Forum, *Building Resilience in Nepal through Public-Private Partnerships*, October 2015, available at http://www3.weforum.org/docs/GAC15_Building_Resilience_in_Nepal_report_1510.pdf.

[4] World Economic Forum, *Resilience Insights*, January 2016, available at http://www3.weforum.org/docs/GRR/WEF_GAC16_Risk_Resilience_Insights.pdf.

[5] David Kirkpatrick, "Now Every Company Is A Software Company," *Forbes,* 30 November 2011, available at http://www.forbes.com/sites/techonomy/2011/11/30/now-every-company-is-a-software-company/#6b5986091100, accessed 17 September 2016; see also Marc Andreessen, "Why Software Is Eating the World", *The Wall Street Journal*, 20 August 2011, available at http://www.wsj.com/articles/SB10001424053111903480904576512250915629460, accessed 17 September 2016.

[6] Jonathan Marino, "Goldman Sachs is a tech company," *Business Insider,* 12 April 2015, available at http://www.businessinsider.com/goldman-sachs-has-more-engineers-than-facebook-2015-4, accessed 9 September 2016.

[7] International Monetary Fund, *Global Financial Stability Report: Responding to the Financial Crisis and Measuring Systemic Risks*, April 2009, p. 113, available at https://www.imf.org/external/pubs/ft/gfsr/2009/01/pdf/text.pdf, accessed 17 September 2016.

[8] See World Economic Forum "Part 1: Global Risks 2014: Understanding Systemic Risks in a Changing Global Environment", available at http://reports.weforum.org/global-risks-2014/part-1-global-risks-2014-understanding-systemic-risks-in-a-changing-global-environment/; and G. G. Kaufman and K. E. Scott, "What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It?" in *Independent Review* 7 (3): 371–391 (2003), p. 371.

[9] Group of Ten's 2001 definition of "systemic financial risk". For reference, the original full description is: *"*Systemic financial risk is the risk that an event will trigger a loss of economic value or confidence in, and attendant increases in uncertainty about, a substantial portion of the financial system that is serious enough to quite probably have significant adverse effects on the real economy. Systemic risk events can be sudden and unexpected, or the likelihood of their occurrence can build up through time in the absence of appropriate policy responses. The adverse real economic effects from systemic problems are generally seen as arising from disruptions to the payment system, to credit flows, and from the destruction of asset values." See Group of Ten, *Report on Consolidation in the Financial Sector*, January 2001, p. 126, available at http://www.bis.org/publ/gten05.pdf.

[10] See World Economic Forum "Part 1: Global Risks 2014: Understanding Systemic Risks in a Changing Global Environment", op. cit.

[11] International Monetary Fund, *Global Financial Stability Report*, op. cit., p. 112.

[12] International Telecommunication Union, *ICT Facts and Figures 2016,* June 2016, available at http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf.

[13] The digital economy contributed $2.3 trillion to the G20's GDP in 2010 and an estimated $4 trillion in 2016, and it is growing at 10% a year – significantly faster than the overall G20 economy. See Boston Consulting Group Perspectives, "The Infrastructure Needs of the Digital Economy", March 2015, available at https://www.bcgperspectives.com/content/articles/telecommunications_public_sector_infrastructure_needs_digital_economy/.

[14] McKinsey & Company, McKinsey Global Institute, "Unlocking the potential of the Internet of Things", June 2015, available at http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world.

[15] According to projections from Cisco, by 2019 more than four-fifths (86%) of workloads will be processed by cloud data centres while only about 14% will be processed by traditional data centres. See "Cisco Global Cloud Index: Forecast and Methodology, 2014-2019 White Paper, October 2015, available at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html.

[16] EMC Corporation, "Study Projects Nearly 45-Fold Annual Data Growth by 2020", May 2010, available at http://india.emc.com/about/news/press/2010/20100504-01.htm.

[17] In fact, in 2025, big data will generate revenues of over $122 billion, triple the amount of revenue it generates today, according to the Frost & Sullivan report, *World's Top Global Mega Trends to 2025 and Implications to Business, Society and Cultures*, June 2014, available at http://www.investinbsr.com/ipaforum/wp-content/uploads/Iain-Jawad-IPA-Forum-2014-Presentation.pdf.

[18] Cognitive systems are "a category of technologies that uses **natural language processing** and **machine learning** to enable people and machines to interact more naturally to extend and magnify human expertise and cognition. These systems will learn and interact to provide expert assistance to scientists, engineers, lawyers, and other professionals in a fraction of the time it now takes." See IBM, IBM Research "Why cognitive systems?", available at http://www.research.ibm.com/

cognitive-computing/why-cognitive-systems.shtml#fbid=xF-OVxV1wGm.

[19] International Data Corporation (IDC), "Worldwide Spending on Cognitive Systems Forecast to Soar to More Than $31 Billion in 2019, According to a New IDC Spending Guide", March 2016, available at http://www.idc.com/getdoc.jsp?containerId=prUS41072216.

[20] Ibid.

[21] Around 80% of cybersecurity attacks can be mitigated by basic security practices. See UK Government Communications Headquarters (GCHQ), Department for Business Innovation & Skills (BIS) and Centre for the Protection of National Infrastructure (CPNI), "Executive Companion: 10 Steps to Cyber Security", 2012, available at https://www.cyberessentials.org/system/resources/W1siZiIsIjIwMTQvMDYvMDQvMTdfNDdfMTdfNjMwXzEwX3N0ZXBzX3RvX2N5YmVyX3NlY3VyaXR5LnBkZiJdXQ/10-steps-to-cyber-security.pdf.

[22] Microsoft, "Rethinking the Cyber Threat: A Framework and Path Forward", available at https://www.microsoft.com/en-us/download/confirmation.aspx?id=747.

[23] Mandiant, "M-Trends, 2015: A View from the Front Lines", available at https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html.

[24] Electricity Information Sharing and Analysis Center (E-ISAC), "Analysis of the Cyber Attack on the Ukrainian Power Grid", March 2016, available at http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[25] In one study of potential vulnerability of the US power grid, Lloyd's of London concluded that a significant attack on the north-east grid could result in up to $1 trillion in damages. See Lloyd's report, *Business Blackout: The insurance implications of a cyber attack on the US power grid*, May 2015, available at https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

[26] World Economic Forum, *Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats*, January 2015, available at http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.

[27] See Section 2A, Financial services sector.

[28] See Section 2B, Transportation sector.

[29] US Department of the Treasury and US Department of Homeland Security, *Financial Services Sector-Specific Plan 2015*, available at https://www.dhs.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf.

[30] The current world population of 7.3 billion is expected to reach "8.5 billion in 2030, and to increase further to 9.7 billion in 2050 and 11.2 billion by 2100", according to the UN Department of Economic and Social Affairs, in its *World Population Prospects: The 2015 Revision* report, available at https://esa.un.org/unpd/wpp/publications/files/key_findings_wpp_2015.pdf.

[31] Zurich and Business Continuity Institute (BCI), *Supply Chain Resilience Report 2015*, November 2015, available http://www.riskmethods.net/resources/research/bci-supply-chain-resilience-2015.pdf.

[32] According to Verizon, 15% of companies actively targeted were in the transportation sector. See the *2013 Data Breach Investigations Report* Executive Summary, available at www.eventtracker.com/wp-content/uploads/verizon-data-breach-2013.pdf.

[33] US Department of Homeland Security and US Department of Transportation, *Transportation Systems Sector-Specific Plan 2015*, available at https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf.

[34] Security Affairs, "A cyber attack against the ground computer systems of the Polish flagship carrier LOT grounded more than 1,400 passengers at Warsaw's Okecie airport", 22 June 2015, available at http://securityaffairs.co/wordpress/37997/cyber-crime/hacked-airline-lot.html.

[35] Rock Health, "2012 Digital Health Funding Update", August 2012, available at https://rockhealth.com/digital-health-funding-update/.

[36] Because of these risks, regulations such as the US Health Insurance Portability and Accountability Act require healthcare organizations to implement administrative, physical and technical safeguards to ensure the integrity and privacy of sensitive data. See the US Department of Health and Human Services, Office for Civil Rights, Breach Portal, "Breaches Affecting 500 or More Individuals", available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[37] IBM, "A survey of the cyber security landscape", 2015, available at http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEJ03320USEN.

[38] Estimates based upon the Ponemon Institute's "Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data" suggest breaches could be costing the healthcare industry nearly $6.2 billion. Also, by some estimates, healthcare data are 10 to 50 times more valuable on the black market than financial data, notably because healthcare data frequently include a range of information, from an individual's address and private medical records to credit card information. See Reuters, "Your medical record is worth more to hackers than your credit card", 24 September 2014, available at http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.

[39] See Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, 2007, New York: Random House.

Acnowledgements

World Economic Forum Global Agenda Council on Risk & Resilience

Chair

Kirstjen Nielsen, Senior Fellow, Center for Cyber and Homeland Security, George Washington University, USA; President, Sunesis Consulting, USA

Contributing Agenda Council Members

Victor Meyer, Global Head, Corporate Security and Business Continuity, Deutsche Bank, United Kingdom

Paul Nicholas, Senior Director, Trustworthy Computing, Microsoft Corporation, USA

Nick Wildgoose, Global Corporate Leader, Supply Chain Product, Zurich Insurance Group, United Kingdom

Expert Contributors

Kaja Ciglic, Senior Security Strategist, Microsoft Corporation, USA

Matthew McCabe, US Critical Infrastructure Cyber Leader, Marsh, USA

Jayaraj Puthanveedu, Director, Information & Resilience Risk Management & Regional Head of Business Continuity- APAC, Deutsche Bank, Singapore

Mark Viola, Vice-President and Global Chief Information Security Officer, Henry Schein, USA

Experts Consulted

Dmitri Alperovitch, Co-Founder and Chief Technology Officer, CrowdStrike, USA

Lori Bailey, Global Head, Special Lines, Zurich Insurance Group, Switzerland

Tucker Bailey, Partner, McKinsey & Co., USA

Adam Blackwell, Vice-President International, Development Services Group, and Chair of the Advisory Board, TechTrace, Switzerland

Ricardo Bonefont, Director, Enterprise IT Security and Compliance, Ryder System, USA

Dale Christian, Chief Information Officer, Touchstone ID, USA

Alan Cohn, Of Counsel, Steptoe & Johnson, USA

Anthony V. Dagostino, Executive Vice-President, Cyber/E&O Practice Leader, Willis Towers Watson, USA

Tom Davis, Vice-President, Susan Davis International, USA

John Dragseth, Senior Analyst, Infrastructure Security Policy, Office of Infrastructure Protection Positioning, Navigation and Timing Program Management Office, USA

Matthew Fleming, Professor, Georgetown University, USA

Carl Gahnberg, Policy Adviser, Internet Society (ISOC), Switzerland

Brendan Goode, Global Head, Cyber Security Operations, Deutsche Bank, USA

Phil Harrington, Senior Managing Director, Brock Capital Group, USA

Fred Hintermister, Manager, Electricity ISAC, North American Electric Reliability Corporation, and Vice-Chair, National Council of ISACs, USA

Lawrence Hughes, Assistant General Counsel, American Hospital Association, USA

Adam Isles, Principal, The Chertoff Group, USA

Jamil Jaffer, Vice-President, Strategy and Business Development, IronNet Cybersecurity, USA

Gerry Kane, Director, Cybersecurity Segment, Zurich North America, USA

Andrzej Kawalec, Chief Technology Officer, HP Enterprise Security and Director, HPE Security Research, United Kingdom

Andreas Könen, Vice President of the Federal Office for Security and Information Technology (BSI), Germany

Ed Lazowska, Bill & Melinda Gates Chair in Computer Science & Engineering, University of Washington, USA

John Manners-Bell, Chief Executive Officer, Transport Intelligence, United Kingdom

Kathleen Montgomery, Managing Director, The Chertoff Group, USA

Robert Morgus, Policy Analyst, International Security Program, New America, USA

Jeff Moss, President, DEF CON Communications, USA

Tom Patterson, Chief Trust Officer and Vice-President, Unisys Global Security, Unisys Corporation, USA

Philip Reitinger, President and Chief Executive Officer, Global Cyber Alliance, USA

Stephen Scharf, Managing Director and Chief Security Officer, Depository Trust & Clearing Corporation (DTCC), USA

Fred B. Schneider, Samuel B. Eckert Professor of Computer Science, Cornell, USA

Jan Whittington, Associate Professor, Director Urban Infrastructure Lab, University of Washington, USA

Beau Woods, Deputy Director, Cyber Statecraft Initiative, Atlantic Council, USA

Chantal Worzala, Director, Policy, American Hospital Association, USA

Justin Zeefe, Co-Founder and Chief Strategy Officer, Nisos Group, USA

Development Support

Erica Buege, Associate Consultant, APCO Worldwide, USA

Susannah Malarkey, Senior Technology Advisor, APCO Worldwide, USA

Alec Nadeau, Presidential Administrative Fellow, Center for Cyber and Homeland Security, George Washington University, USA

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