Cybersecurity: a Challenge to Business in the Era of the Fourth Industrial Revolution

Author Naoyuki Haraoka

By Naoyuki Haraoka

Introduction

The Global Risks Report 2016 by the World Economic Forum (WEF) highlights a variety of risks ranging from the global environment to national security and also the Fourth Industrial Revolution that will start to affect our daily business soon. These risks are expected to have a crucial impact on our political economy, business and eventually human civilization overall. Some of them are the result of new technology brought about by the Fourth Industrial Revolution. Since we do not yet have a clear overview of this new technology, even technology experts cannot predict exactly what its impact will be on our social and political economy. At this juncture, however, cybersecurity is the most immediate risk to be considered in this regard.

The WEF's research on global business leaders' views shows that the risk of cyberattacks is one of the largest technology risks in terms of likelihood and impact in several countries, including the United States, Japan, Germany, Switzerland and Singapore, while the risk of the functions of key information infrastructures being damaged and halted is seen to be decreasing *(Chart 1)*.

Cyberattacks feature among the top five risks in 27 economies, according to the WEF, indicating the extent to which businesses in many countries have been impacted already by this rising threat. The WEF report assumes that possible damage brought about by crimes in cyberspace could amount to $445 billion, exceeding the national income of each of the many national economies. It calls for cooperative action from business, governments and academia to boost the resilience of societies to withstand this risk.

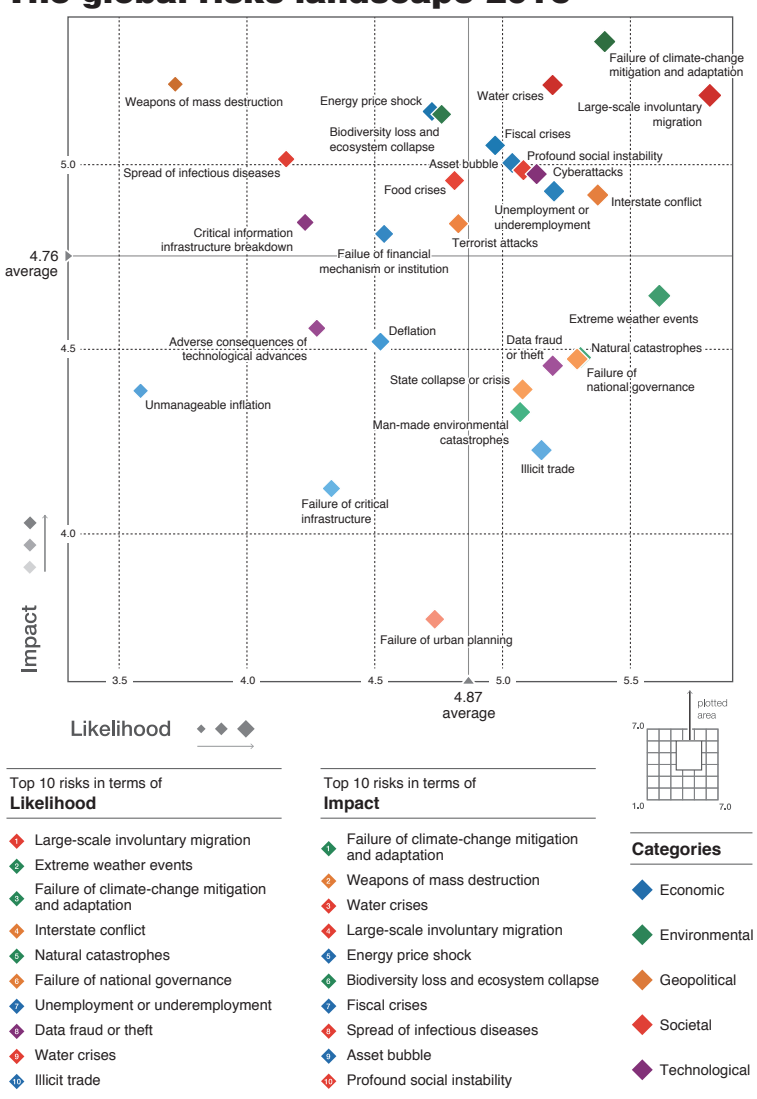
To achieve this, social stability and cooperation is critical. It is noteworthy in this context that our digital economy could create a digital divide between citizens empowered by technology to access highly detailed information and networks and others feeling they are being discriminated against by those so empowered. This could create conflicts and social instability.

Benefits & Risks of Internet-related Technologies

Many hope that emerging technologies will fuel a new wave of productivity and growth. A recent study suggests that Internet-related

CHART 1

The global risks landscape 2016



Top 10 risks in terms of **Likelihood**

- Large-scale involuntary migration
- Extreme weather events
- Failure of climate-change mitigation and adaptation
- Interstate conflict
- Natural catastrophes
- Failure of national governance
- Unemployment or underemployment
- Data fraud or theft
- Water crises
- Illicit trade

Top 10 risks in terms of **Impact**

1. Failure of climate-change mitigation and adaptation
2. Weapons of mass destruction
3. Water crises
4. Large-scale involuntary migration
5. Energy price shock
6. Biodiversity loss and ecosystem collapse
7. Fiscal crises
8. Spread of infectious diseases
9. Asset bubble
10. Profound social instability

Categories

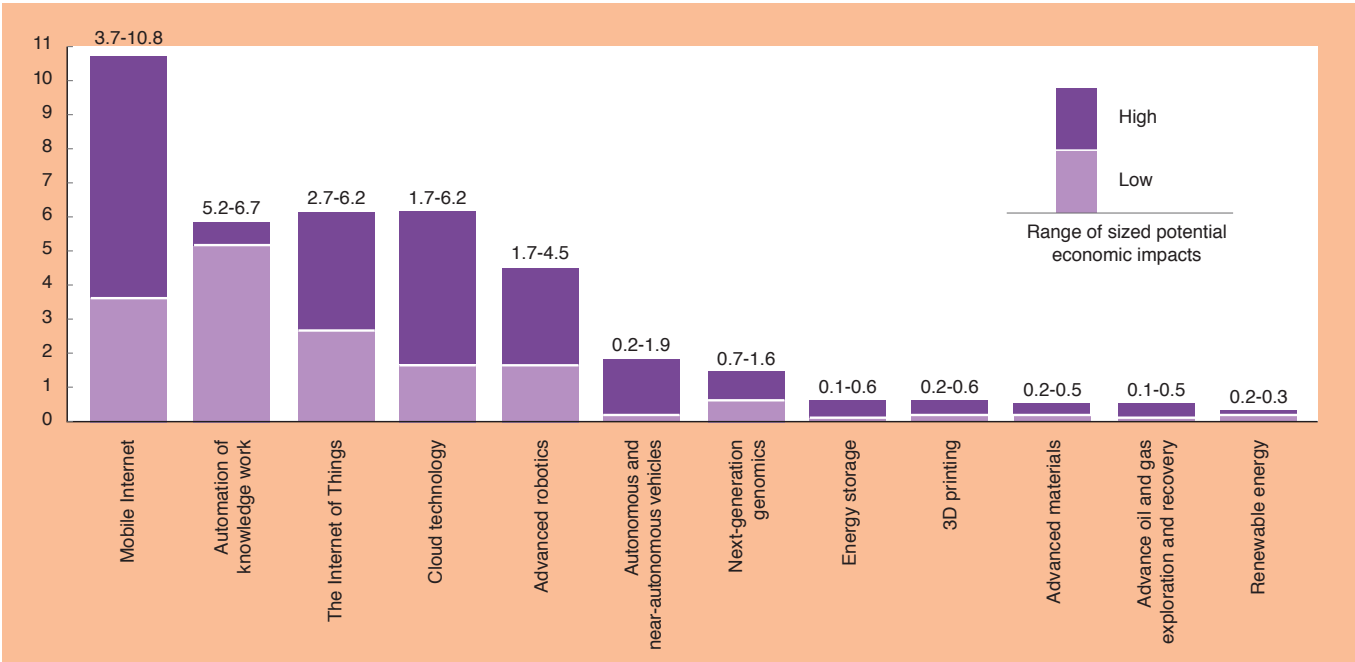
- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Notes: Survey respondents were asked to assess the likelihood and impact of the individual risks on a scale of 1 to 7, 1 representing a risk that is not likely to happen or have an impact, and 7 a risk that is very likely to occur and have massive and devastating impacts.

Source: Global Risks Perception Survey 2015, World Economic Forum

CHART 2

Estimated potential economic impact of technologies ($ trillion, annual)



Note: Projections are to 2025 and include sized applications and consumer surplus.
Source: Based on Manyika et al. 2013, World Economic Forum

technologies such as mobile Internet devices, the automation of knowledge work, the Internet of Things (IoT) and cloud technology will be the most disruptive and generate the most economic benefit *(Chart 2)*.

Meanwhile, the failure to understand and address risks related to the systemic cascading effects of cyber risks or the breakdown of critical information infrastructures could have far-reaching consequences for national economies, economic sectors and global enterprises. By one estimate, European nations, if they fail to react appropriately to technological change, could lose 600 billion euros over the next 10 years, corresponding to about 10% of Europe's industrial base. Thus we will need to address correctly the following four high-level risks associated with the transformation towards a more digitized economy, as mentioned in the WEF report.

First, as the IoT leads to more connections between people and machines, cyber dependency will increase, raising the odds of a cyberattack with potential cascading effects across the cyber ecosystem. As cyber dependence rises, the resulting interconnectivity and interdependence could diminish the ability of organizations to fully protect their enterprises. As more organizations move to digitize their unique business value within more connected environments relying increasingly on machine learning, cyber resilience takes on a new importance. They will need to invest appropriately to enhance operational risk management and strengthen organizational resilience. It is vital to integrate physical and cyber management, strengthen organizational and business processes, and leverage supporting technologies.

Second, assuming that data will be "the oil of the 21st century", a predictable legal framework is needed to realize the full economic potential of digitization. We will need an international legal framework complementing national governance in areas such as privacy, transparency, encryption control, the effect of intellectual property regimes on data crossing borders, and the impact of proprietary data on competition. The existing lack of certainty about the legal situation could hamper investment and adaptation of the latest technologies. Moreover, the physical infrastructure for data exchange such as undersea cables could also become a target in international conflicts or terrorism.

Third, although there is a lot of uncertainty about how many new types of jobs new technologies will create and what they may be, it is likely that more existing categories of jobs will be replaced by computers. One estimate is telling us that 47% of US jobs are potentially automatable over the next decade or two. For example, robots will take over manual tasks in online retail stock keeping, healthcare and diagnostics, as well as checking in hotel guests. Knowledge workers performing non-routine cognitive tasks could be displaced by advances in intelligent algorithms. The entire employment system may have to be re-thought to facilitate transitions between different types of jobs. For human beings, skills in STEM (science, technology, engineering and mathematics) are considered important in the medium term, with longer-term needs projected to focus on skills such as creativity, problem-solving and social intelligence. Education systems must be redesigned in the long run to focus on skills where humans can still be expected to outperform machines, such as teamwork, interaction, relationships and cultural sensitivity. In a more automated future, value will come from emotional and contextual

intelligence.

Businesses will need to invest more in the continuous learning, re-skilling and up-skilling of their employees as well as talent management in order to complement such redesigned education systems. In addition, governments must look beyond education systems to redesign the broader enabling environment for talent by interventions across a person's lifetime, such as regulatory support for entrepreneurship.

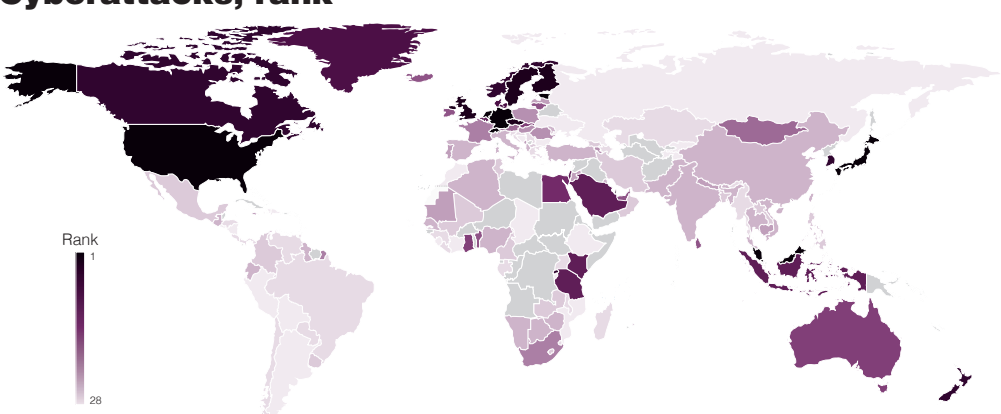
Fourth, access to technology is likely to exacerbate income differences within and across countries, with those who adapt gaining and those who do not losing income. Four billion of the planet's 7 billion people still do not have access to the Internet and may not be able to gain from technology-driven growth. Advancing technology could diminish returns to labor and lead to wealth accumulating in fewer hands. Excessive inequality lowers aggregate demand and threatens social stability.

Current Situation of Cyberattacks

Cyberattacks are already an existing threat. From personal finances to business operations and national infrastructure, public and private services and amenities are increasingly managed via some form of computer network and are consequently vulnerable to attack. Recent technological advances such as the IoT have been beneficial in many respects, but they have opened the door to a growing wave of cyberattacks, including economic espionage, cybercrime and even state-sponsored exploits. *Chart 3* shows us the regions in the world where cyberattacks are frequently observed. A sharp increase in high-profile cases has been continuing and shows no sign of slowing down. Cyberattacks are today also involving major powers such as the US, Russia and China, and can be regarded as political incidents. In the spring of 2016, the computer system of the Central Bank of Bangladesh was invaded by a hacker and 9.1 billion yen was illegally remitted, while in September it was discovered that there had been a leakage of the personal information of 1.5 billion people from Yahoo USA. There is a suspicion that Russia could be involved in both cases.

CHART 3

Cyberattacks, rank



Note: The darker the colour, the higher the concern.
Source: Executive Opinion Survey 2015, World Economic Forum

According to Akamai Technologies Inc., the leading US content delivery network services provider, the share of China as the origin of distributed denial of service (DDoS) attacks, a cyberattack by sending a mass of information to a specific server and causing it to crash, was around 30% of total DDoS attacks during July-September in 2016, while the share of the US was 20%, that of the United Kingdom 15%, and France less than 10%. China and Russia are taking aggressive strategies to expand their presence in cyberspace by enabling private citizens to carry out cyberattacks on their behalf against public entities as well as private business to acquire a political advantage. For example, it is said that they have obtained necessary information on the weapons of other nations by these cyberattacks.

Cyberattacks are occasionally used as a means to transfer a message to their targets. For example, cyberattacks have been used to declare the intention to oppose Japanese whaling. A DDoS was the principal method of attack and it was not only the whaling business but also media and publication offices that were the victims of those attacks. We also often see cyberattacks related to sports events. The oldest one was at the Asia Cup football tournament in 2004 hosted by Japan, when the Japan Football Association and sponsoring companies had their websites attacked. Japanese government offices and media companies were also targeted. At the Euro 2008 football championship UEFA suffered a large-scale DDoS attack on its official website.

Much time and effort was spent in preparing countermeasures against possible cyberattacks on the occasion of the Beijing Olympics in 2008, the World Cup in 2010, and the London Olympics in 2012, on the assumption that a big sports event could be an easy target for cyberattacks as it would be on air or on websites so often and a cyberattack would be an effective means of issuing a political message to the world.

Cyberattacks could damage the functions of important social infrastructures. The large-scale blackout in Ukraine in December 2015 was thought to have been caused by cyberattacks. According to an Executive Opinion Survey 2015 by the WEF, a cyberattack is perceived as the risk of highest concern in eight economies: Estonia, Germany, Japan, Malaysia, the Netherlands, Singapore, Switzerland and the US. The 2015 Fortune 500 CEO survey found that cyber security came second when CEOs were asked about their companies' biggest challenges.

The WEF Global Risks Report 2016 says that attempts to detect and address attacks are made harder by their constantly evolving nature, as perpetrators quickly find new ways of executing them. Businesses trying to match this speed in their development of prevention

and response methods are sometimes constrained by a poor understanding of the risk, a lack of technical talent, and inadequate security capabilities. Although CEOs worry about rising cyber risks, the ownership of and responsibility for cyber risks is less clear. Who in a corporation is the actual owner of the risk? While there are many "C" level owners (CISO, CFO, CEO, CRO, Risk Management), each of these has differing but related interests and unfortunately often does not integrate risk or effectively collaborate on its management. Defining clear roles and responsibilities for cyber risk is crucial.

According to the WEF, outdated laws and regulations inhibit governments' ability to capture criminals but also to expedite the often lengthy procedure of elaborating and implementing legal and regulatory frameworks to reflect evolving realities. The sophisticated threats of government-sponsored economic espionage also exceed the defensive capabilities of many commercial enterprises, which are more and more frequently looking to other governments to intervene. The G-20 recently took an unexpected, but applauded, step and collectively affirmed "that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."

Businesses are increasingly accepting the fact that they cannot hope to prevent all cyberattacks. The difficulty in preventing attacks is not outmatched by the difficulty in identifying and effectively mitigating them. Given the types of vulnerabilities utilized by attackers and their methods, many attacks and intrusions are not immediately discovered — some are recognized only months and in some cases years later. The emphasis needs to be on streamlining mechanisms for early detection, response and recovery, to mitigate and better manage the consequences — limiting the damage, and ensuring business continuity.

The WEF report stresses that it will also become clearer that cybercrimes cannot be fought unilaterally. Although businesses can follow standard industry practices or adopt individually tailored ways to deal with cybercrimes, cooperation throughout the value chain (because attacks can be made through supplier systems) and with law enforcement should be also helpful. As is often the case, however, public-private partnerships can be held back by lack of trust and misaligned incentives. Businesses may fear exposing their data and practices to competitors or to law enforcement agencies. And the private sector's primary interest in rapid recovery and continuity of business operations may not align with the public sector's primary interest in apprehending and prosecuting perpetrators. In addition, governments need to balance their investments in offensive cyber weapons and efforts to enhance capabilities for cybersecurity and defense.

Future Outlook for Cybersecurity

The WEF report on global risks 2016 has a special chapter on the Security Outlook 2030. It says that technological innovation as well as social fragmentation and demographic shifts will accelerate transformative shifts in political and economic power, and that will have a crucial impact upon the international security order. One of the most salient examples is that the powers in the world would drift into major conflict as they dispute responsibility for a devastating cyberattack on crucial infrastructure, ultimately resulting in a reworking of a stripped-down global system. The international security landscape is likely to be profoundly affected by not only information technology enabling us to utilize cyberattacks but also revolutionizing technologies changing the nature of conflict from autonomous weapons systems to 3D-printed weaponry and even to genetically engineered biological weapons. Understanding these changes and formulating responses to the risks they represent will be essential for leaders when contemplating the years ahead towards 2030.

The scope of cyberattacks could also expand in the coming years, if a shortage of qualified cybersecurity personnel, the slow pace of development of cybersecurity rules, and insufficient coordination efforts between companies and government organizations are not correctly resolved. Following the success of Russia's recent cyber-enabled influence operations, the risk of other governments exploiting weak cybersecurity practices across a wide range of private and academic institutions is increasing. As IoT progresses further in society, we will need to accelerate our efforts to eliminate the lag in regulatory responses at both national and international levels to alleviate the risks of catastrophic breakdowns of key Internet infrastructure empowering IoT devices. It is also true that as concerns about terrorist activity grows in the future, there will be an increasing need to access smart devices, since for terrorist investigations the police will need more encrypted data. This could conflict with customer privacy. How to mitigate this conflict between security and privacy will be another issue that will need to be settled in the future.

Conclusion to WEF Global Risks Report

Addressing global risks lies beyond the capacity of individual businesses. Businesses need to strengthen their resilience to ensure continued operation and survival in the face of risks. At the same time, the clear role for collaboration among public and private sector actors becomes evident, for example, to develop better cybercrime prevention methods, to establish cybersecurity norms for both governments and industry, and to align international approaches to enforcement and establish industry norms. Above all, it is in the key interest of businesses to find new ways to partner with governments to address global risks. Many risks, ranging from energy security to unemployment, can only be addressed through diverse stakeholders recognizing the need for joint action. Such collaboration requires the identification of key risks and related interests, and strong alignment and robust agreement among business and other stakeholders on the need to address them.

National governments and all private businesses, as well as international organizations, must share a sense of crisis to achieve proper cybersecurity in line with this conclusion. JS

Naoyki Haraoka is executive managing director and editor-in-chief of Japan SPOTLIGHT.