Fujitsu's Engagement on Cybersecurity in Supporting a Connected Society

● Kentaro Mukai

Innovative digital technologies, such as cloud computing, big data, AI, and IoT are now familiar to us, and the digitalization of society is accelerating. A "connected society," formed by connecting all things such as people and things with data, is affecting the structure of social and economic systems and dramatically changing our daily lives. Digital innovation has brought us a "connected society" and is now advancing the digitalization of customers' business environments and businesses in an unstoppable manner. As these changes bring improved convenience, at the same time, we are confronted with emerging new threats, causing cybersecurity to become indispensable in protecting systems and data. Cybersecurity has now become the core foundation of Fujitsu's every business, and we recognize that is our mission to sustain our capability in cybersecurity to keep earning customer's trust. This paper describes Fujitsu's approach on cybersecurity in support of a connected society.

1. Introduction

In Japan, smart speakers have a low penetration rate of only 3–5%, and I myself have been uneasy and hesitant about inviting this somewhat strange digital assistant into my home. However, the news[1)] that the penetration rate in the United States has exceeded 40% gave me the reason to give it a try. The new life with the smart-speaker is unexpectedly comfortable and it somehow gives the feeling that the future has arrived to our household.

The future that we dreamed about in the 20th century is now becoming a reality thanks to innovative digital technologies such as AI, IoT, cloud computing, big data, blockchain technology, mobility, robotics, and the soon-to-launch fifth generation mobile communications system (5G).

The Japanese government proposed "Society 5.0"[2)] as the society of the future that aims to put technologies and data to good use against the backdrop of an expanding digital society. This society can only become a reality, however, with cybersecurity. From here on, we can expect digital innovation to accelerate and life to become all the more convenient through a "connected society" formed by connecting all kinds of things to data. At the same time, new threats to economic activities and daily life are arising in society.

At Fujitsu, we consider cybersecurity to be the means of supporting core business operations, and with this in mind, we are accelerating our initiatives in supporting our customers from now and into the future as they come face to face with this transition to a digital society.

This paper describes Fujitsu's cybersecurity initiatives in support of a connected society.

2. Global trends and current cyber threats

This section describes global trends, the present state of cyber attacks, and the measures taken by governments in dealing with the situation.

2.1 Global trends

Taking a broad look at global trends since 2018, it can be seen that nationalism in the form of a "my country first" approach is on the rise, and that trade wars between the superpowers are intensifying. At the same time, there is an increasing trend toward exclusivity on a global scale, the international order shows signs of wavering, and geopolitical risks are on the rise. Perhaps as a result of this state of affairs, uneasiness in economic matters is beginning to appear. For

example, the International Monetary Fund (IMF) announced in October 2018 that world economic growth was slowing down for the first time in several years and that inflation was accelerating.

Technological trends and the wave of digital innovation are also beginning to affect the international cooperation system. Discussions on data protection are already taking place on the global level, including talks on restricting cross-border transfers of specific types of data. In addition, the "singularity" that AI is expected to trigger, 5G that will increase communication speeds by 100 times, and digital technologies such as quantum computing will foster innovation and most certainly bring about dramatic changes not only to our daily lives but also to the battlefield and war itself. In the long term, dominance in the field of digital technology is directly connected to dominance in the world, so conflict among the superpowers over their stake in this field is likely to continue.

In "Top Risks 2019," the Eurasia Group, known for its analysis of geopolitical risks, raised the possibility of Western countries taking more aggressive deterrence methods such as "hack back" and raising "Cyber gloves off" as third in the top ten global risks.[3] In short, concern about cyber wars is growing–geopolitical, economic, and technological trends are becoming intricately entwined, generating conflict between nations. It is feared that such conflict will become more intense from here on, and that the outlook for the international community and the world economy will become increasingly opaque.

2.2 Intensified cyber attacks

The perpetuators of cyber attacks range from individuals to national organizations. The total number of cyber attacks in Japan increased dramatically by 12.4 times from 2013 to 2018.[4] In addition, worldwide economic damage due to cyber attacks rose to approximately 600 billion dollars in 2017,[5] which came to approximately 15% of the 4 trillion dollars[6] of total corporate net profit for that year.

Our society is facing "new threats" amid the trend toward increasing digitalization. In 2017, the ransomware[note 1] known as WannaCry spread throughout the world in as little as 24 hours inflicting damages in the real world to hospitals and factories, railway ticket vending machines, etc. Other notable cyber attacks include the large-scale power outage in the Ukraine in 2015 (attack on a social infrastructure), theft of virtual currency in 2017 (attack on a financial system), and suspicious manipulation of information in the United States presidential election of 2016 (assault on democracy).

From here on, a variety of countries including developed nations will become targets. Long-term suspension of critical social infrastructures such as financial and power systems may endanger human life, and there is concern that a cyber attack may give rise to systemic risk as in the 2008 financial crisis.

2.3 Evolution of attack techniques

Cyber attacks have been intensifying accompanied by rapidly evolving attack techniques. Malware such as NotPetya and SamSam appeared within only a few years after WannaCry, and variants of each continued to evolve. Ransomware code has even been used to mine for virtual currency. Recent years have also seen the appearance of "fileless malware," which is undetectable by existing antivirus software. This type of attack makes use of memory or genuine tools (PowerShell, WMI-Windows Management Instrumentation, etc.) installed in a Windows terminal.

Targeted attacks have been traditionally mounted by techniques that use e-mail, websites, or USB memory, but there have also been cases using other means such as chatbots or Wi-Fi hacking. Attack techniques are becoming increasingly clever as reflected by attacks that embed a backdoor in the software or hardware of manufacturing processes within supply chains or that distribute malware by exploiting regular software update functions.

Although attention has generally focused on the means of countering malware-oriented attacks or targeted attacks, there has also been a rise in unauthorized access using illegally obtained user authentication information to impersonate a valid user, in attacks that exploit vulnerabilities in web applications, and in theft of information from electronic commerce (EC) sites.

The technologies generated by digital innovation is expanding the attack surface (areas of targets). Innovative digital technologies include smartphones,

note 1) Malware that takes data or a system hostage and demands a ransom in exchange. Malware is software that includes malicious intent.

IoT, and operational technology (OT), and more recently, AI. For example, there are concerns about attacks that could induce erroneous judgments in AI by contaminating training data. The Cyber Kill Chain model proposed by Lockheed Martin Corporation in 2011 described the seven phases of a cyber attack. At present, however, approximately 90% of all attacks are now executed with the first five steps collapsed into a single action,[7] which reflects the increasing sophistication of techniques on the attack side.

Taking the above into consideration, new countermeasure frameworks are being developed such as MITRE ATT&CK[8] and the Cyber Threat Framework[9] of the US Government.

2.4 Recognizing and countering threats

As threats continue to expand, it was recognized for the first time at the Davos Forum[note 2] in January 2018 that cyber attacks constitute one of the three major risks for corporate managers. Continuing on, the same forum in 2019 ranked cyber attacks as one of the top five risks that have a high likelihood of occurring.[10] The following summarizes the background to recognizing cyber threats as a primary management issue:

- Cyber attacks continue to inflict damage on many companies and threaten management.
- Global governance and the implementation of countermeasures are difficult.
- Complying with the many laws and regulations on cybersecurity (in relation to data, supply chains, cloud computing, IoT, etc.) in each country or region is difficult.

In addition, the following unique characteristics of cyber attacks make dealing with them difficult:

- Difficulty in identifying attributions
- Residence of the attackers (being overseas)
- Implications of foreign state actors in attacks
- Defense being the only option for business entity
- Difficulty in establishing deterrence
- Difficulty in dealing with internal threats
- Limit in cybersecurity talent pool
- Overwhelmingly disadvantaged situation for the defenders

In the United States, crisis awareness of cyber attacks targeting the supply chains of ICT products is taking hold, and hi-tech products having latent risk are being excluded from government and critical-infrastructure procurement. Japan as well is being pressed to deal with such cyber attacks accordingly from the viewpoint of national security. The National Institute of Standards and Technology (NIST) of the United States is working to incorporate supply chain risk management (SCRM) requirements in existing standards and guidelines and to disseminate countermeasures to cyber attacks. These security requirements will surely become an "admission ticket" to the market, and if product-and-service providers and even users should be late in complying with those requirements, they may be forced to exit the market. In the United States, the Department of Homeland Security announced in November 2018 the formation of its ICT Supply Chain Risk Management Task Force to strengthen coordination between the public and private sectors.[11]

3. Solutions supporting a connected society

In response to these issues, Fujitsu aims to continue supporting digital innovation that its customers need for growth by striving to minimize the negative (minimize the customer's business risk from cyber attacks) and maximize the positive (support digitalization as an aggressive investment by the customer, etc.) as a strategy in the cybersecurity business (**Figure 1**).

This section describes the solution group provided by Fujitsu, key areas of focus, and differentiating elements.

3.1 Life-cycle-based solutions

Fujitsu provides solutions encompassing the entire life cycle of cybersecurity as a one-stop service (**Figure 2**). The following summarizes the key functions of these solutions.

1) Assessment and consulting

Fujitsu provides security consulting on the customer's system and business design with business continuity into account. This includes assessments, such as vulnerability analysis and business-impact analysis. It also includes vulnerability improvement and resistance enhancement of various process and

note 2) The annual meeting of the World Economic Forum held in Davos, Switzerland in January. Attended by political and business leaders and scholars from countries around the world.

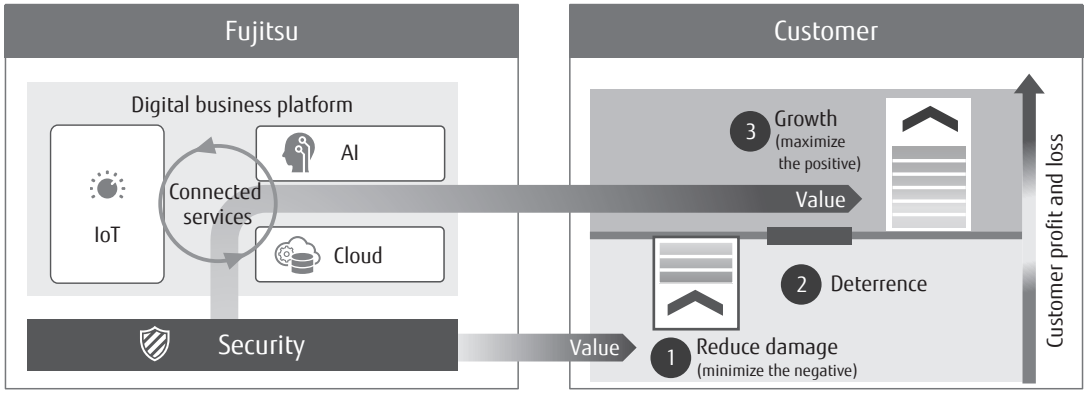

Figure 1
Fujitsu's cybersecurity business model.

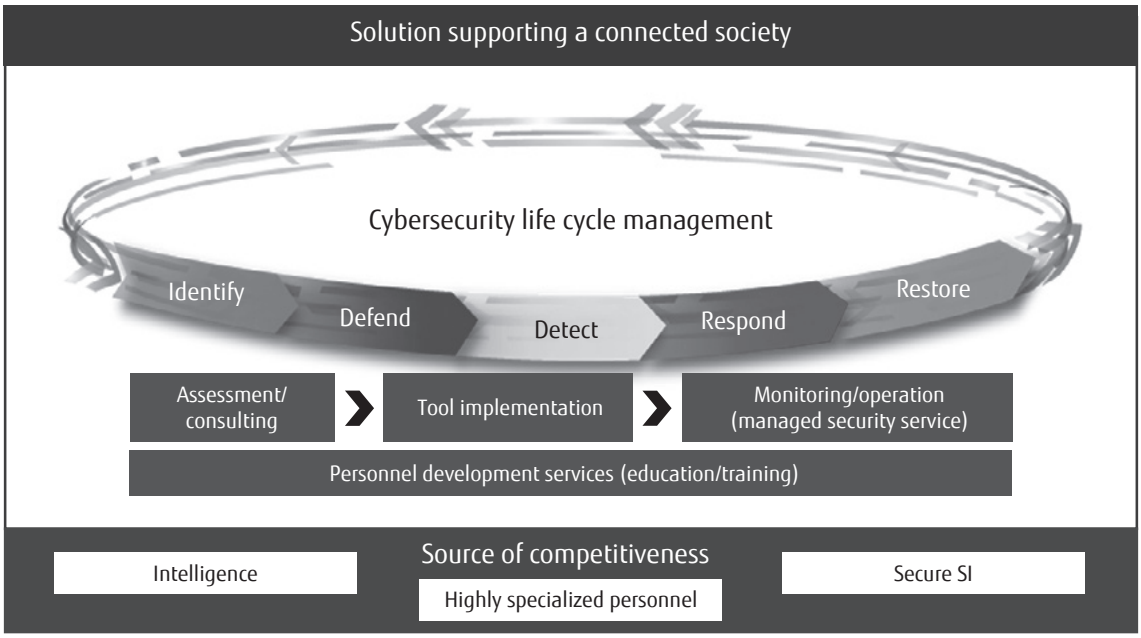

Figure 2
Life-cycle-based solutions and source of competitiveness.

systems.

2) Tool implementation

This function achieves secure system integration (SI) by implementing security requirements and constructing a secure system.

3) Monitoring and operation

Fujitsu provides a managed security service (MSS) that performs 24/7 real-time monitoring and operation of cybersecurity across the entire system including the customer's personal computers and networks. It features life-cycle-based handling of cyber attacks from defense to detection and proactive response as well as strengthening of operations and incident response.

4) Personnel development services

These are education and training services for developing highly specialized security personnel.

Using solutions with the above functions, Fujitsu provides the following four elements as a one-stop service on a global basis. These elements combined reflect Fujitsu's comprehensive strength and competitive edge.

- Source of differentiators

Diverse types of security-related intelligence, highly specialized security personnel, cutting-edge technologies and services, and business infrastructure including Security Operation Center (SOC)

- Understanding customer's environment and business

Use of knowledge accumulated over many years at system-operation sites

- Application of security requirements to systems (secure SI)

Application of integration skills backed by a security design incorporating requirements from the system planning stage

- Global coverage

Global support through a two-headquarter system in Tokyo and London

3.2 Essential intelligence

As described in Section 2, geopolitical, economic, and technological global trends are thought to have a major social impact even in cyberspace. In addition, Fujitsu collects and analyses intelligence from around the world such as laws and regulations and standards/specifications related to security, threat information related to cyber attacks, etc., and applies this intelligence to our services.

Since there are no organizations that are exempt from cyber attacks or that can completely prevent penetration, attacks are dealt with on the basis of a reactive model in which a response is taken place after the occurrence of an incident. As a result, attacks continue until detection of the penetration. According to a recent survey, the time from the occurrence of a cybersecurity breach to detection is 101 days as a world average, but as many as 498 days in the Asia-Pacific region.[12] These figures reflect the need for speeding up "detection" and "post-detection response."

At Fujitsu, we aim to minimize damage by reducing the period from breach to detection by supplementing the conventional "incident-driven approach" with an "intelligence-driven approach." The idea behind this approach is to minimize damage by reading signs of a threat in advance, enhancing defensive capabilities in a timely manner, achieving early detection, and promoting countermeasures with related departments. These measures also contribute to system restoration through proactive defense and immediate response that take into account business continuity for the customer (**Figure 3**).

As for information on cyber threats, the Advanced Artifact Analysis Laboratory (A3L) established within Fujitsu collects and analyses the latest information from the Internet, dark web, etc. and performs malware, digital forensics, and incident analyses. It also shares threat information stored in a database to strengthen security services.

Against the background of heightened global interest in cybersecurity, all sorts of security-related regulations and standards are being established in countries and regions throughout the world. Under these circumstances, Fujitsu is making a conscious effort to understand not only the specific content of these

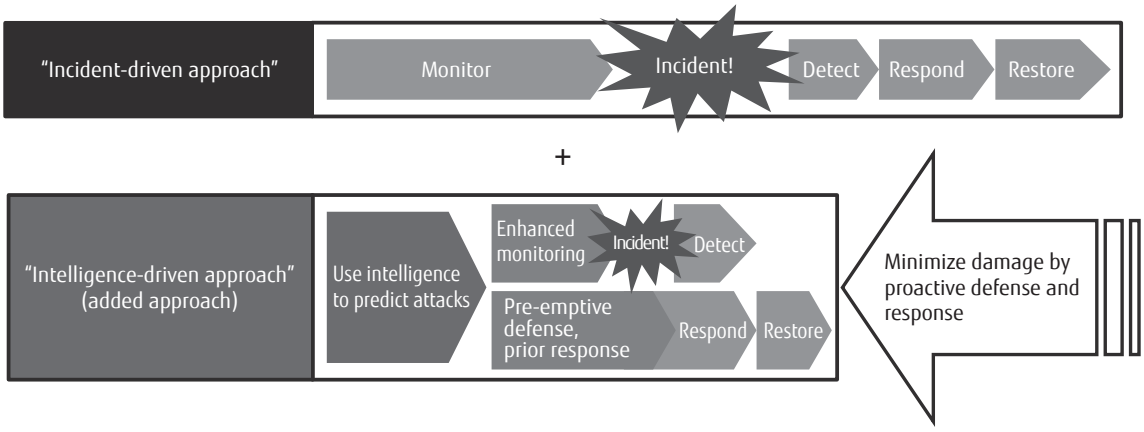

Figure 3
Intelligence-driven security.

regulations and standards but also the background to their establishment so that they can be reflected quickly in Fujitsu's business operations.

To support a variety of systems in the ever-changing world of digital business, it is essential that we be vigilant about future threats that have yet to manifest and to continually refine the quality of our intelligence. By combining this intelligence with knowledge accumulated over many years at system-operation sites, Fujitsu is committed to providing its customers with extensive support.

3.3 Secure SI

"Security by design" is essential to incorporating cybersecurity measures in systems. To thoroughly implement security by design, Fujitsu established Enterprise Security Architecture (ESA) in 2006 to provide basic technical guidelines on in-house information security measures.

In ESA, Fujitsu defined solution architecture (standard framework, operation techniques, technologies, and products) and released an ideal Security Management Framework (SMF). Fujitsu considers that a secure SI business can make its customers aware of Fujitsu's value.

Digital innovation brings with it an explosive increase in targets that must be protected, from people, data, and IoT to all sorts of facilities. And thus, the borderline of cybersecurity is becoming increasingly vague. To deal with such changes in the environment, Fujitsu has set out to revise the existing ESA. The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) proposed "security by design" in 2011 as a policy for ensuring information security from the planning and design stage.[13] In line with this movement, Fujitsu is spreading a "security by design" approach through in-house highly specialized cybersecurity personnel or "Security Meisters."

3.4 Highly specialized personnel

Fujitsu established its Security Meister Certification System as a mechanism for cultivating essential talent to counter cyber threats on a permanent basis. The plan is to train as many as 11,000 in-house highly specialized personnel by the end of FY2021.

Fujitsu is training personnel to give them the practical abilities to mount an appropriate initial response to incidents and to interface with security specialists. Furthermore, with the aim of promptly delivering the solutions that customers need, Fujitsu is also training a specialized sales force consisting of sales personnel having specialized knowledge and experience to lead efforts in solving customer issues in a variety of industries and business fields.

In addition to such in-house training, Fujitsu is also undertaking the training of security engineers in collaboration with government, industry, and academia.

4. Advanced technologies supporting a connected society

A connected society is made up of data, systems, people, AI, IoT, etc. To protect the society of the future, cybersecurity technologies that can guarantee the reliability of each of these constituent elements are indispensable.

Enabling the safe data transfers among various entities during its life cycle is essential. Following are some of the technologies necessary from the viewpoint of the data protection.

- Technology enabling secure access to data
- Data anonymization and encryption technologies to minimize risk even in the case of data leaks
- Blockchain technology as a means of data management to prevent data tampering

There is also need for measures that can deal with various types of risk such as preventing data fed to AI from becoming contaminated.

Digital innovation has advantages for the attacking side as well. In the future, advances in AI will no doubt lead to automatic and high-speed attacks mounted without human intervention. This means that the defending side will not be able to cope unless it itself continues to innovate. For this reason, Fujitsu has begun work on automation and orchestration techniques to speed up and enhance complex security operations.

Furthermore, with the aim of developing new services centered on proprietary technologies, Fujitsu is moving forward with the following initiatives.

1) Advanced MSS technologies

- Threat detection: Endpoint Detection & Response (EDR), Managed Detection & Response (MDR), threat hunting
- Identity and access management: Identity Access Management (IAM), Identity Governance &

Administration (IGA)
- Platform: Threat Intelligence Platform (TIP), automation and orchestration techniques
- Application of AI to the above

2) Data-reliability protection technologies
Fujitsu's proprietary ConnectionChain technology
3) Quality enhancement (testing technologies)
Technologies for detecting unknown vulnerabilities in systems and IoT products (fuzzing tools)
4) Authentication (biometric authentication technology)
5) IoT/OT security
6) Data protection technologies, encryption, etc.

5. Fujitsu's security vision

Fujitsu established a dual-headquarter system in Tokyo and London in 2018 to further strengthen security services including MSS. This will accelerate our efforts in providing advanced-technology services. We will also continue our efforts in improving our services through multi-region support, advanced business infrastructures such as SOC, and security intelligence applications. Additionally, given the prime importance of securing talents in supporting these operations, we will enhance our security-training techniques making maximum use of Fujitsu's global system.

Through collaboration with industry, government, and academia including our customers, partner companies, and specific industrial fields, Fujitsu is committed to fortifying its cybersecurity ecosystem on a global scale.

6. Conclusion

This paper described new threats accompanying digital innovation and Fujitsu's cybersecurity initiatives in support of a connected society.

Cyber attacks will not cease as long as cyberspace continues to be a platform for human activities and value creation. Cybersecurity is essential to the development of a safe and secure society. At Fujitsu, earning the trust of our customers is paramount, and we will continue to confront these attacks with all our technical capabilities.

References

1) RBC Capital Markets Report: Tech Crunch (2018).
https://techcrunch.com/2018/12/28/smart-speakers-hit-critical-mass-in-2018/
2) Government of Japan: The 5th Science and Technology Basic Plan.
https://www8.cao.go.jp/cstp/english/basic/5thbasicplan.pdf
3) Eurasia Group: Top Risks 2019.
https://www.eurasiagroup.net/files/upload/Top_Risks_2019_Report.pdf
4) National Institute of Information and Communications Technology (NICT): NICTER Analysis Report 2018 (in Japanese).
http://www.nict.go.jp/press/2019/02/06-1.html
5) McAfee & CSIS: "Economic Impact of Cybercrime—No Slowing Down" (2018).
https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf
6) Nikkei: "Global Corporate Net Profit Increases by 30% in FY2017—Four Chinese Companies in Top 10." (in Japanese).
https://www.nikkei.com/article/DGXMZO29489060X10C18A4MM8000/
7) Alert Logic: 2018 Critical Watch Report.
https://www.alertlogic.com/resources/industry-reports/2018-critical-watch-report/
8) MITRE: ATT&CK.
https://attack.mitre.org/
9) Office of the Direction of National Intelligence: Cyber Threat Framework.
https://www.dni.gov/index.php/cyber-threat-framework
10) World Economic Forum: The Global Risks Report 2019.
http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
11) Department of Homeland Security: DHS Announces ICT Supply Chain Risk Management Task Force Members.
https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members
12) FireEye: M-Trends 2018.
https://content.fireeye.com/m-trends/rpt-m-trends-2018
13) National Center of Incident Readiness and Strategy for Cybersecurity: Security by Design (in Japanese).
https://www.nisc.go.jp/active/general/pdf/SBD_overview.pdf

Kentaro Mukai
Fujitsu Ltd.
Mr. Mukai is currently engaged in development of global business.