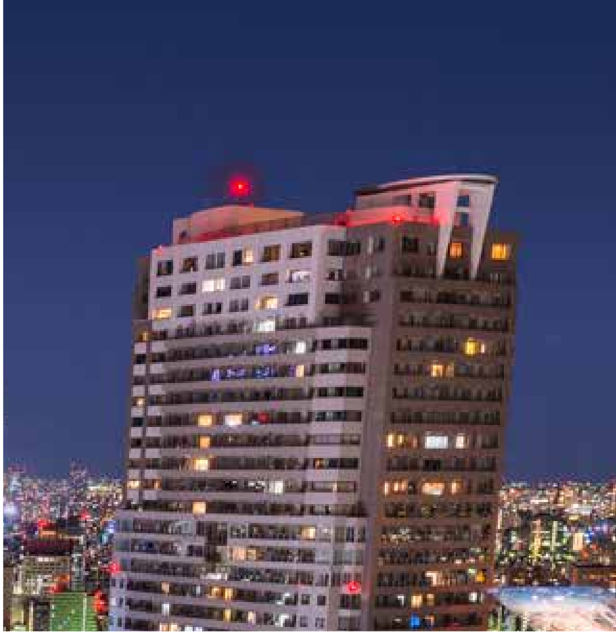


2021 Cyber IQ Survey

The shift toward proactive security

pwc

www.pwc.com/jp

Table of contents

Introduction

The trend of digital transformation (DX) is sweeping both the public and private sectors, and it has become clear that business operations and IT will become even more closely intertwined in the future. As a result, we expect the importance of cybersecurity to further increase. Cybersecurity will become essential not only for organisations to protect their information assets and ensure business continuation, but also to enhance their corporate value by gaining the trust of society and customers.

In the PwC Japan Group's 2021 Cyber IQ Survey conducted of 262 Japanese security leaders, we conducted a fact-finding investigation on the current and three-year outlook for security strategy, planning, structure, investment, supply chains, threat intelligence, privacy, and other fields. This report, which summarises the findings of the survey, contains valuable insights for security leaders in Japan.

We hope that our recommendations based on these survey results will help your companies to take effective security measures.

PwC Japan Group Cyber Security Co-Leader

Taiji Ayabe
Partner, PricewaterhouseCoopers Aarata LLC

Kei Tonomura
Partner, PwC Consulting LLC

About the 2021 Cyber IQ Survey
The 2021 Cyber IQ Survey was conducted among leaders and decision-makers of security organisations in companies with sales of 50 billion yen or more in a wide range of Japanese industry sectors, and received 262 responses.
This survey was conducted by the PwC Japan Group in June 2021.

1. Trends in changes surrounding cybersecurity at Japanese companies

Connections between digitised business and IT supply chains

In September 2021, the Japanese government established the Digital Agency with the mission of ‘boldly promoting future-oriented digital transformation (DX) as the command centre for the formation of a digital society’[1]. DX has become a major social concern and government-led initiative; we see this abbreviation almost every day. It is only natural, then, that in the business sphere, DX is no longer just an initiative of a few large, advanced businesses. Businesses of all sizes and industries are devoting their energy to business transformation based on digital technology.

While the advancement of DX is accelerating the use of digital technologies such as cloud, AI, IoT, and blockchain at various companies, it is already well-known that the importance of security is increasing as a measure to ensure the safe use of these technologies. The importance of cybersecurity for digital connection is also rapidly increasing as the number of companies working on DX and digitalisation has further increased.

Digital connection can be viewed from two perspectives: that of the business supply chain and the IT supply chain.

The business supply chain refers to a series of value-providing activities from procurement to sales. In the case of the manufacturing industry, for example, stakeholders include various companies such as suppliers of raw materials and components, contractors for manufacturing and engineering, and distributors and dealers.

Companies also have a wide variety of internal stakeholders, including overseas offices, subsidiaries, factories, and laboratories. As DX and digitalisation progress, systems will be linked among multiple entities. For example, the company that owns the system and other companies, the company’s domestic and overseas offices, its headquarters and factories, and its processes and data flows will be organically connected. While this is expected to increase the efficiency of the entire supply chain and improve the value provided, it also increases security risks throughout the supply chain. In fact, many cyberattack incidents originate from outsourcing business partners or overseas office locations whose security measures are not as advanced as those of the head office, through system and network connections[2].

The IT supply chain is a chain of outsourced IT systems and services[3], including not only outsourced system operation and maintenance (O&M), but also cloud services such as infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Many companies have been outsourcing their IT-related operations and shifting to the cloud, which has brought various benefits. However, if the provider of such services suffers a security violation, the damage may spread to all companies using the services. Therefore, security risks in the IT supply chain are also increasing.

[1] Digital Agency. ‘About us’. (https://www.digital.go.jp/about)
[2] ENISA. ‘Threat Landscape for Supply Chain Attacks’. (https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks)
[3] Information-technology Promotion Agency, Japan (IPA). ‘Regarding “The Survey Report on the Scope of Information Security responsibility in IT Supply Chain”’. (https://www.ipa.go.jp/security/fy30/reports/scrm/index.html#L)
Reference: PwC. ‘Cyber intelligence: Examples and countermeasures against software supply chain attacks spreading around the world’. (https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/cyber-intelligence07.html)

The acceleration of 'zero trust' in the wake of the COVID-19 pandemic

Another phenomenon that has brought about drastic changes in the business environment today is the rapid change in working styles, including the shift to remote working, due to the outbreak of COVID-19, which has been ongoing since early 2020. Many companies have made, or are currently making, various efforts to reinforce their IT infrastructure, including the installation and expansion of business terminals and VPNs, and to strengthen the associated security systems. In the early days of the COVID-19 pandemic, many companies gave priority to implementing and expanding their VPNs, putting off vulnerability measures and other security measures. As a result, cyberattacks that exploited the vulnerabilities of VPNs were rampant[4]. However, there has been some progress in reducing these attacks by addressing the vulnerabilities on the corporate side. On the other hand, with the rapid spread of remote working in addition to the ongoing shift to cloud computing, and with the prospect that such new working styles will be maintained to some extent in a post-COVID-19 era, companies are now facing an even greater turning point: the need to evolve from the 'perimeter defence model'.

The 'perimeter defence' approach to security is to clearly delineate the inside and outside of the network with firewalls and other systems, and to protect the inside of the network from threats on the outside. However, as more and more business operating systems are moved to cloud environments, and employees become able to access these systems from a variety of environments including their homes and rented offices as well as from their company offices, this concept of separating the inside and outside of the network is becoming increasingly inviable.

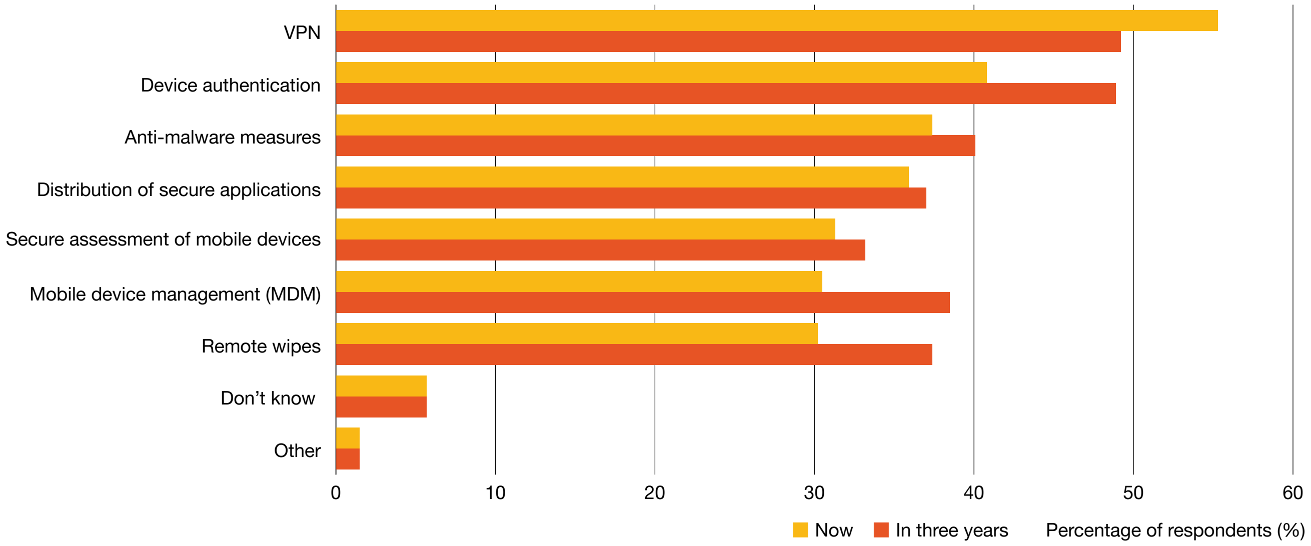
In this context, the concept of 'zero trust architecture' (ZTA) has begun to attract considerable attention. As the name indicates, 'zero trust' refers to the idea of not trusting anything unconditionally. Technically, ZTA is achieved by performing detailed authentication and authorisation based on the identity and context of users and devices, regardless of the network they are connected to. ZTA itself is a concept that has existed since before the COVID-19 pandemic, but with the recent changes in working styles, this concept is becoming more necessary and urgent. However, because ZTA is just an architectural concept and not something that can be achieved by installing a specific security solution, even many advanced companies are now facing barriers and issues and exploring various possibilities.

The Cyber IQ Survey results showed that perimeter defence measures such as VPNs were still the most commonly deployed measures for mobile devices. (55.3% of respondents selected 'VPN' as the security measure they use for mobile devices, the largest percentage of all options.) (See Figure 1.)

Meanwhile, regarding security measures that respondents have already taken and are planning to take in the next three years, survey results showed that ZTA-related measures such as risk-based authentication, multi-factor authentication, and single sign-on (SSO) are likely to increase, suggesting that companies are willing to change their mindset. However, in reality, the shift to ZTA is difficult to achieve in a short period of time, and we therefore expect companies to proceed in an incremental manner with the maturation of the related product markets and migration of current assets. (See Figure 2.)

Figure 1: Security measures for mobile devices that companies have implemented (and are considering implementing in the next three years)

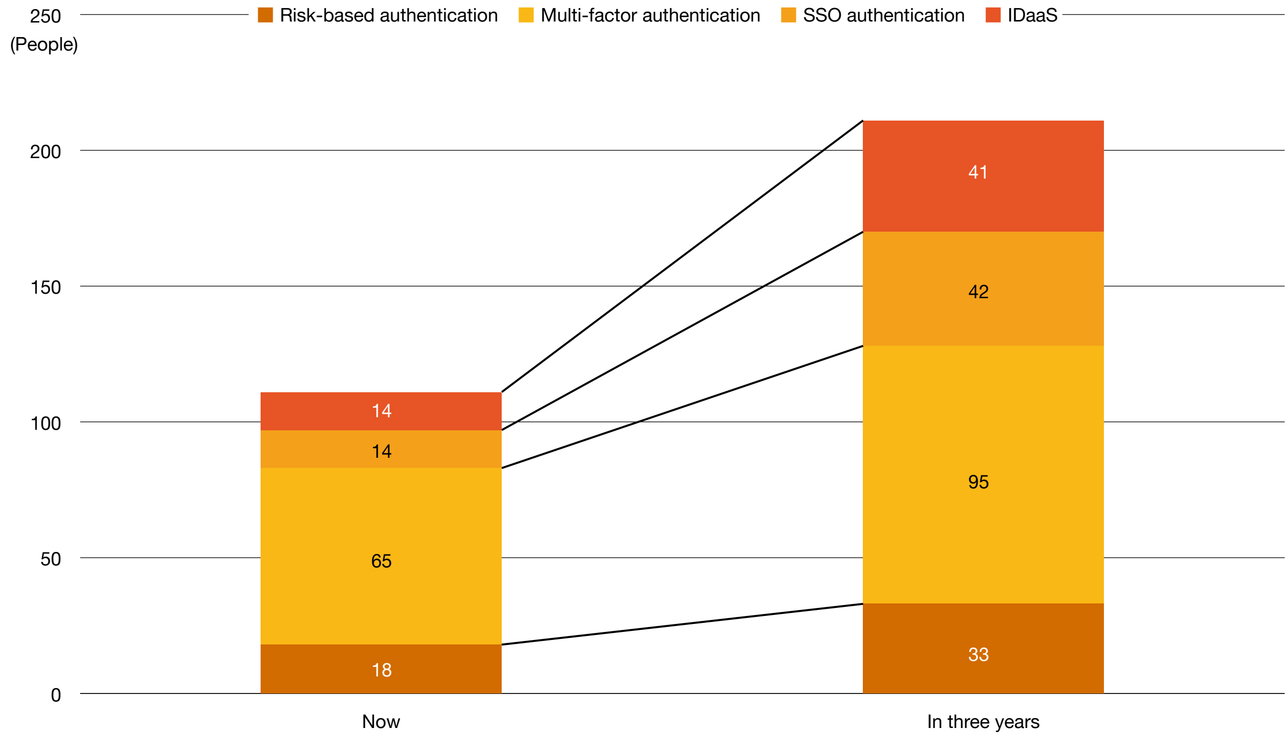
Q) Please select the security measures you are currently taking, and that you expect to be taking in three years for your mobile devices. (Select all that apply.)



[4] CISA. 'Alert (AA21-209A) Top Routinely Exploited Vulnerabilities'.(https://us-cert.cisa.gov/ncas/alerts/aa21-209a)

Figure 2: ZTA-related security measures that companies have implemented (and are considering implementing in the next three years)

Q) Do you plan to significantly increase your adoption of ZTA-related solutions such as risk-based authentication, multi-factor authentication, and SSO and IDaaS in the next three years?



Related links:
PwC: ‘Next-generation IT infrastructure: Zero trust architecture—Changing role of IT infrastructure and the suitability of zero trust’. (https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture01.html)
PwC. ‘Survey on “zero trust architecture” in Japanese businesses 2021’. (https://www.pwc.com/jp/ja/knowledge/thoughtleadership/zero-trust-architecture-survey2021.html)

The rise of 'multiple extortion ransomware'

In addition to changes in the business environment, cyber threats are also constantly changing. One cyber threat that has attracted particular attention in the last few years is ransomware. Ransomware is a type of malware, and WannaCry, which spread rapidly in 2017, and Emotet, which was prevalent from 2019 to 2020, are still fresh in our memories. In the 2021 edition of the annual report '10 Major Security Threats' published by the IPA, 'Financial Loss by Ransomware' is listed as the number one threat for organisations.

The typical ransomware attack pattern is that the attacker infects the target system with the ransomware, encrypts the data so that it cannot be used by the user, and demands a ransom payment for the decryption of the data. When a company is infected with ransomware, the availability of its systems and data is compromised, and depending on the affected systems, the company might be forced to cease operations or even business itself. As such cases have become widely known, many companies have taken countermeasures by backing up their systems and data and developing rapid recovery processes in case of emergency.

In recent years, however, a new attack pattern called 'double extortion ransomware', which cannot be dealt with by such countermeasures, has become widespread. The term 'double extortion' refers to a 'two-stage' extortion scheme: the traditional ransom demand by encrypting the data, and the leakage of the stolen confidential and personal information if the demand is not met.

As a more urgent scenario, some ransomware has adopted a time-limited extortion method; leaking part of the stolen data on the dark web and leaking the rest of the data if payment is not made within 72 hours. Furthermore, some ransomware has also been found to use triple-stage extortion, sending a large amount of communication data to the victim organisation's website and interfering with the operation of the website if the ransom is not paid. The pressure to pay the ransom is increasing, and ransomware attacks have become increasingly more malicious.

In this way, cyber threats continue to change both in terms of attack methods and their usage, and the reality is that attackers and companies are in a cat-and-mouse game. In order for companies to reduce cyber risks as much as possible, it is vital to keep abreast of cyber threat trends and continue to review countermeasures based on flexible and broad assumptions of risk scenarios. In addition, security measures must be taken not only to protect against threats, but also to detect security breaches in a timely manner and to make organisations resilient so that they can promptly respond and recover from them. Particularly, in such a risk scenario resulting from ransomware attacks, the damage will affect the continuity of operations and business, and the company will need to make a decision on whether or not to pay the ransom. Therefore, it will be especially important to develop a response and recovery process that involves stakeholders throughout the business, including management, legal and communications divisions.

Related link: PwC. 'Cyber intelligence: The threat of double extortion ransomware increases with the introduction of remote working'. (https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/cyber-intelligence06.html)

The maturing cyberattack business

The spread of ransomware and the expansion of threats as explained on the previous pages is likely due to the fact that cyberattacks have become a business and a service, typified by ‘Ransomware as a Service’ (RaaS). RaaS, as the term implies, is a system that provides the necessary tools and know-how for ransomware attacks as a service. In 2021, an incident occurred in which ransomware provided by a RaaS group called DarkSide forced a large company to temporarily suspend its operations.

The RaaS service model is very similar to the Software as a Service (SaaS) model; ransomware developers offer their services to users who wish to use them by charging them a fee in the form of licensing or on a pay-per-performance basis. Of course, the market for such ‘dark services’ is not usually accessible through ordinary web browsers and search engines, but in the ‘deep web’, which can only be accessed through special software and channels. These areas of the web do not necessarily exist for the purpose of cyberattacks or cybercrime, but they have become a place for such ‘dark services’ to thrive because they are difficult for ordinary users to detect and are highly anonymous.

Although special methods are necessary to access the deep web, the barriers are not as high as creating cyberattack tools and know-how by oneself, thus creating a situation where even those who don’t have advanced knowledge and skills can conduct cyberattacks in a relatively easy way. In addition to the provision of services necessary for cyberattacks, the distribution and sale of target information such as IP addresses and authentication information necessary for attacks, and the recruitment of corporate insiders to participate in attacks are conducted in the deep web. The market for cyber threats is considered to be growing and maturing, supported in part by the popularity of cryptocurrency, which is convenient for anonymous payments.

In summary, cyber threats continue to evolve to outsmart corporate countermeasures, and the hurdles to launching an attach are becoming lower and lower as the market for attack tools and know-how matures. At the same time, companies must continue to pay close attention to internal threats such as internal fraud and inadvertent leaks, in addition to external threats. It is crucial for companies to recognise that they are unfortunately facing a growing number of these threats and to continuously review their countermeasures.

Related: link: PwC. ‘Cyber intelligence: The threat of double extortion ransomware increases with the introduction of remote working’. (https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/cyber-intelligence06.html)

Businesses are increasing resilience, but still have a long way to go

The environment in which businesses operate is rapidly changing due to the use of information and IT as well as digitalisation and DX in recent years. And cyber threats, such as ransomware, are also evolving. Amidst these circumstances, it has been a long time since the concept of 'cyber resilience' has been proposed as an essential strategy for corporate security measures. (See PwC's The Global State of Information Security Survey 2018.) The term 'resilience' means elasticity or capacity to recover. The purpose of cyber resilience is to focus on minimising the impact of cyberattacks on business operations and quickly returning to normal, as it has become practically impossible to completely prevent cyberattacks. If we apply this concept to the five functions of the US National Institute of Standards and Technology's Cyber Security Framework (NIST-CSF), 'Identify', 'Protect', 'Detect', 'Respond' and 'Recover', we can say that the purpose of cyber resilience is to focus on the entire process from detection to recovery, not just on protection.

So to what extent are companies actually improving their cyber resilience? In this survey, we asked which of the five NIST-CSF Functions was the most important for security measures and found that 'Protect' (41.2%) and 'Detect' (35.9%) received a large number of responses, while 'Respond' (5.0%) and 'Recover' (5.3%) were far behind. When asked how they see the situation three years from now, the percentage of respondents who answered 'Protect' remained almost the same at 39.7%, while the percentage of those who answered 'Detect' decreased significantly to 21.4%. On the other hand, the percentages of respondents who answered that 'Respond' and 'Recover' were the most important were 19.1% and 10.3% respectively, indicating that the focus of corporate countermeasures is gradually shifting (Figure 3).

These survey results show that while many companies are willing to focus not only on protection but also on detection and recovery to enhance their resilience, they have not been involved in response and recovery. Despite the prevalence of the concept of cyber resilience, businesses still have a long way to go to realise it.

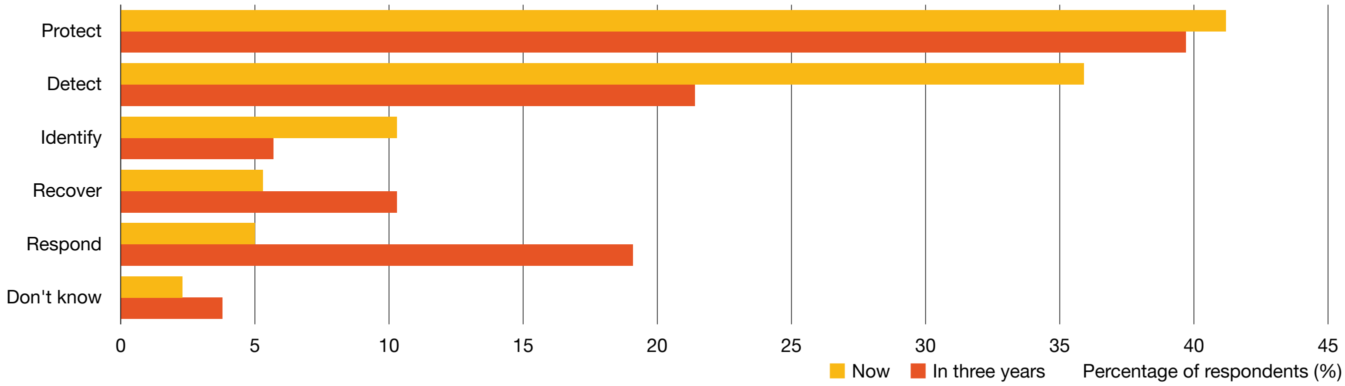
While companies are struggling to secure their resilience, cyber threats continue to expand. As mentioned previously, there have been many reports of ransomware and other malware attacks entering the networks of other parties in the supply chain or remote workplaces, leading to security incidents. In addition to the office environment, the environments of production and research locations such as factories have also become digitalised, and those systems are now connected to each other by networks. This is why the intrusion of a cyber threat can lead directly to the disruption of an entire business and its operations, and why the damage caused by security incidents is becoming more and more serious.

In this survey, when asked how they were affected by security incidents that occurred in the past year, the percentages of respondents who answered, 'Systems down' and 'Business impact' were 22.5% and 19.8% respectively, along with 'Data breach' at 21.8% (Figure 4).

Regarding 'Business impact', many respondents reported impacts directly related to business and operational continuity, such as 'disruption of business, processes and services' (26.9%) and 'network strain' (26.9%) (Figure 5).

Figure 3: Security functions that companies consider most important (currently and in the next three years)

Q) Which of the five NIST-CSF Functions ('Identify', 'Protect', 'Detect', 'Respond' and 'Recover') is the most important for security measures, and which do you think will be the most important in three years?



In summary, cybersecurity risks are becoming a greater threat to the continuity of business and operations, similarly to the threat presented by information leaks. They are also becoming increasingly important as a management issue. As far as changes in the business environment and cyber threats are concerned, the severity of such impacts is expected to continue to accelerate. So, how should companies fight against this risk? Of course, it remains important to have a strategy that aims to improve resilience rather than to pursue perfect protection. However, as cyber risks have become a greater threat to business continuity and an incident can now have fatal consequences, such a strategy is no longer sufficient. The next generation of security measures will require a shift from the 'reactive' approach of preparing for emergencies with all-round protection against invisible threats to the 'proactive' approach of understanding threats in a proactive manner and changing countermeasures dynamically and flexibly.

Figure 4: Impact of security incidents suffered by companies

Q) How has your organization been impacted by security incidents? (Select all that apply.)

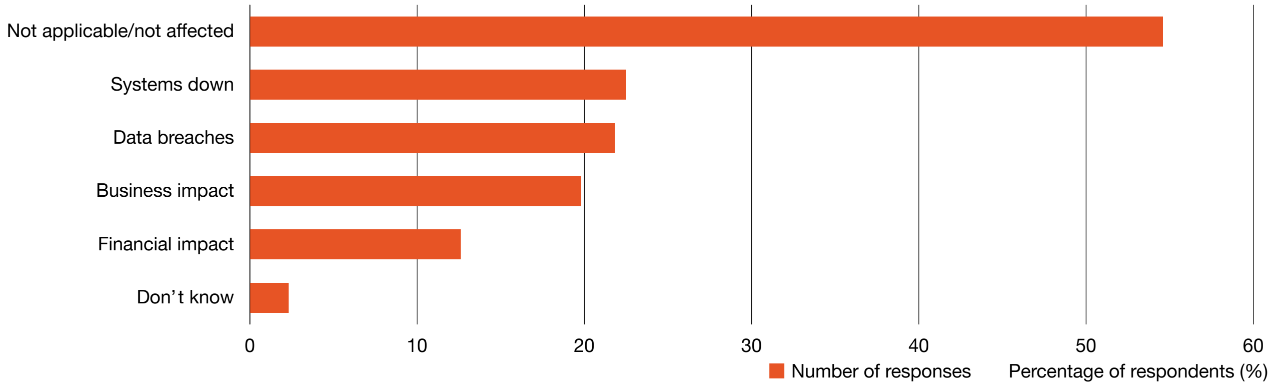
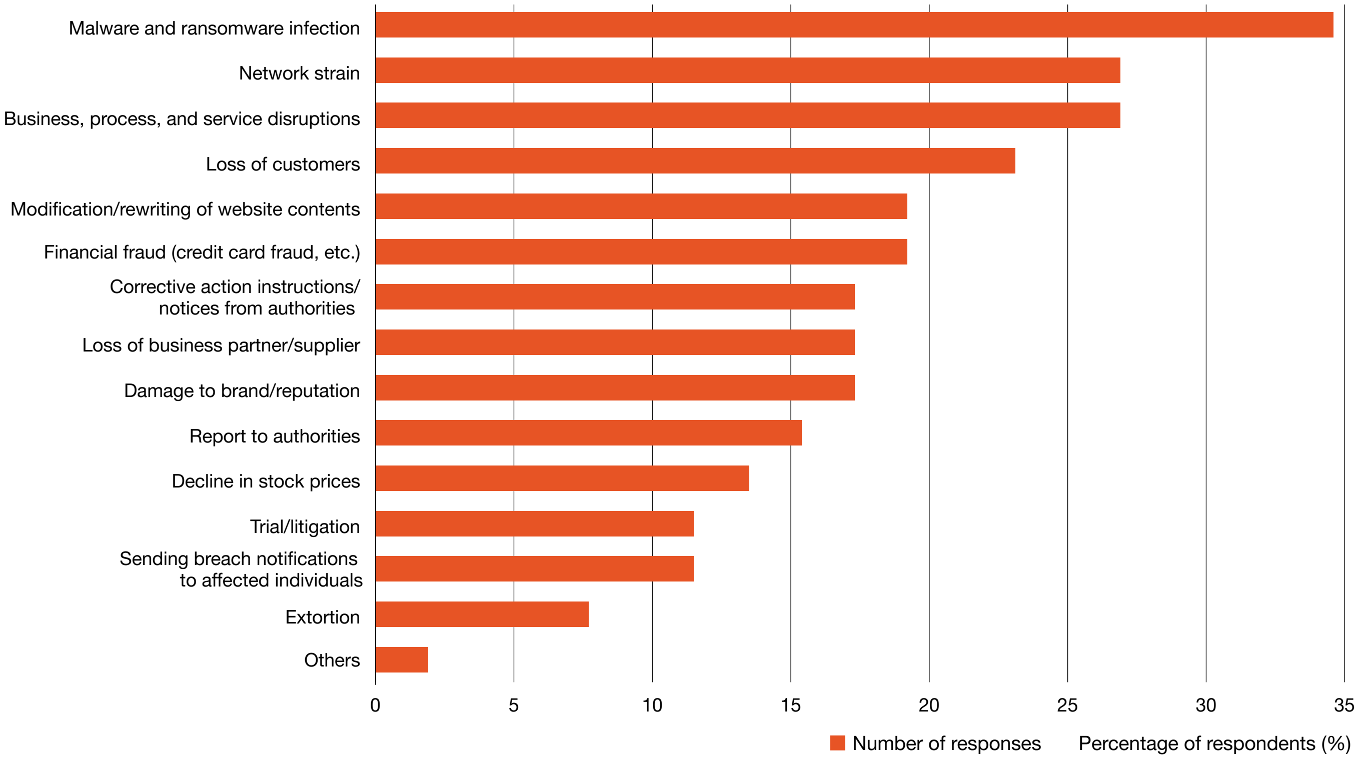


Figure 5: Business impact of security incidents

Q) For those who selected 'Business impact' in the previous question. What kind of impact have you experienced?



Related link: PwC. 'Preparing for cyber shock and strengthening the digital society'. (https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2018/assets/pdf/strengthening-digital-society-against-cyber-shocks.pdf)

2. The shift to proactive security

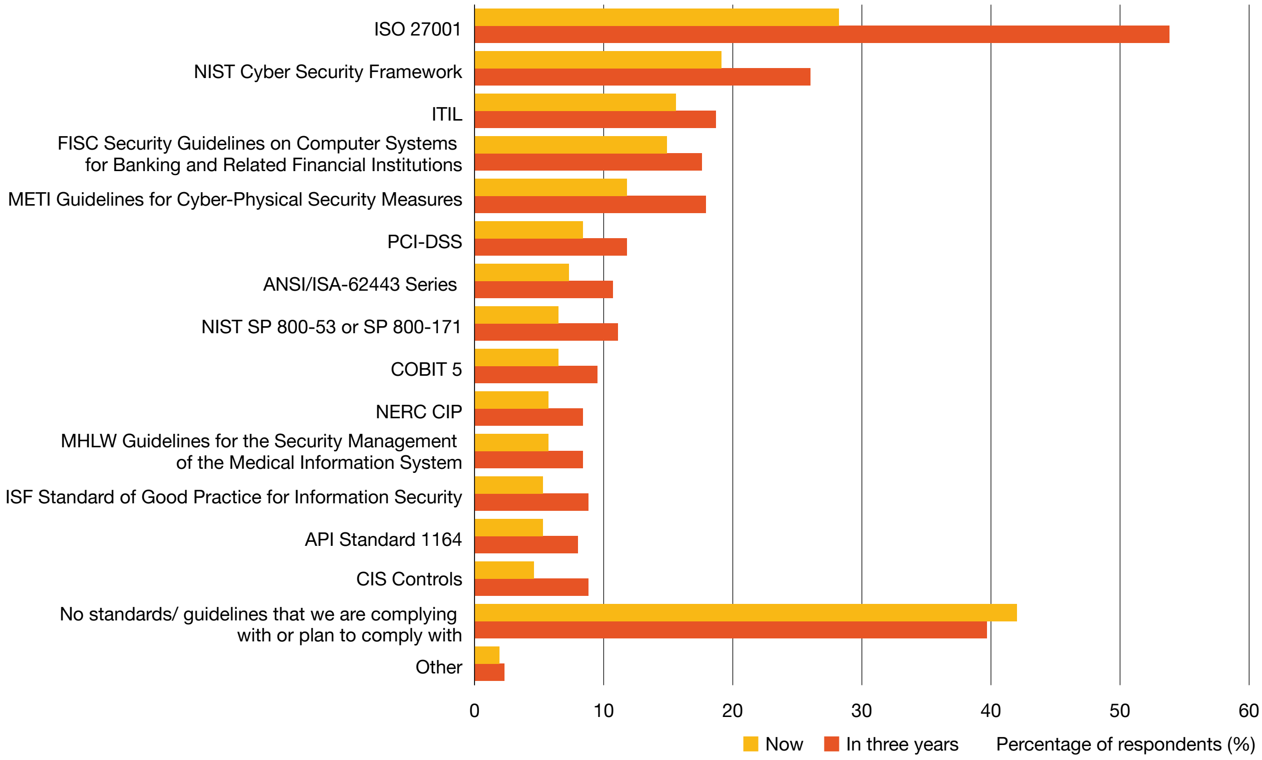
As mentioned in the previous chapter, with recent changes in the business environment and cyber threats, it is becoming difficult for companies to fight against the latest cyber threats by simply promoting security measures through traditional approaches. By 'traditional approaches', we mean conducting assessments based on security standards and guidelines, and developing and promoting security response plans based on identified and prioritised gaps and issues. In this survey, when asked about the standards and guidelines they are currently in compliance with, 28.2% of the respondents selected 'ISO 27001', followed by 'NIST Cyber Security Framework' at 19.1%. When asked about their outlook for the next three years, these figures rose to 53.8% and 26% respectively, showing high compliance rates (Figure 6).

However, these standards and guidelines are the results of studies and formulations based on the paradigm at a certain point in time, and it is inevitable that there will be gaps between the standards and guidelines and the latest paradigm as time passes from the time they were published and enforced. Furthermore, in order to combat the new cyber threats that emerge every day, companies need to assess the risks and review their response plans as soon as they become aware of new cyber threats. These approaches are known as the 'baseline approach' and the 'risk-based approach'. What today's companies need, however, is 'proactive security', which is a further development of these two approaches.

Architectural changes such as cloud migration and the rise of supply chain risks have both expanded and blurred the areas which companies need to protect. Cyber attackers are tactically exploiting these new risks to conduct cyberattacks. Therefore, it is essential that companies collect and analyse not only internal information but also external information, including information on the intentions and capabilities of cyber attackers, in order to avoid a situation where they are attacked from an unexpected direction, only to find it is too late. By collecting and analysing this information, it becomes possible to predict possible threats to the organisation with a high degree of accuracy and prepare for them. Performing such a series of activities in a near-real-time cycle is 'proactive security'. In order to achieve such security governance without being overwhelmed by daily risk assessment, it is important to define security management items as a common language across the organization and to establish systems and processes for measurement, improvement, and reporting.

Figure 6: Standards and guidelines that companies are currently in compliance with (and are considering compliance within the next three years)

Q) Are there any standards or guidelines that your company currently complies with or plans to comply with in the next three years? (Select all that apply.)



Specific actions to achieve proactive security

So what kind of efforts will companies need to take to achieve 'proactive security'? In addition to their current efforts to develop and promote security response plans, companies will need to collect and analyse external factors related to cyber risks in order to acquire and strengthen capabilities to deal with urgent risks and to dynamically review their plans. This is the basic concept.

Currently, a revision of ISO 27002, which will incorporate best practices related to ISO/IEC 27001, is underway, and it is expected that 'threat intelligence' will be added as a new requirement. This move is in line with the concept of proactive security, and companies that operate information security management systems based on ISO 27001 can therefore consider incorporating this activity into their current systems and processes as one approach. Organisations that have established an active computer security incident response team (CSIRT) can expand and redefine the roles and functions of the CSIRT and add the relevant functions. Various implementation methods are possible, depending on the organisation of the company

When asked about the status of their threat intelligence efforts, about 80% of the respondents said that they collect data by themselves or via outsourcing. In addition, when asked how they are using the data, 'Input for strategy formulation' and 'Input for incident response' topped the list at 45.1%, while 'No specific use, but refer to it as needed' and 'Don't use it much' were both selected by 37.7% of the respondents. These results indicate that companies face challenges in using the collected data (Figure 7). In light of these survey results, the key to achieving proactive security is figuring out how to make the collected data usable. In this section, we will describe specific recommended actions based on typical issues faced by Japanese companies.

1. Identify KSFs of the business that could be affected by cyber risks.

Traditionally, cyber risks have been recognised as IT system risks and were considered to be owned and managed by the information systems division. However, recent cyber risks are not only a risk to IT systems but also a management issue directly related to business continuity, as we've described in the previous sections. Listed companies in particular are encouraged to disclose the status of their cyber security measures in their annual securities reports[5], and perceptions of cyber risks are starting to change.

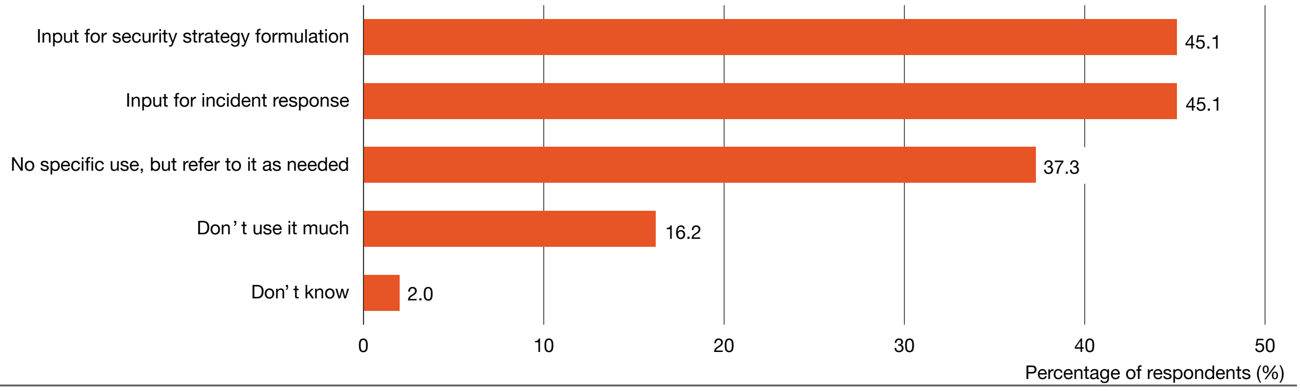
However, even if data on cyber risks is collected, analysed, and reported at the management meeting, it will be difficult for companies to make effective decisions unless the correlation between cyber risks and their impact on business can be clearly explained. Therefore, companies need to examine key success factors (KSFs) for business continuity and identify in advance the factors that are affected by cyber risks. This will allow businesses to consider whether and to what extent any recognized cyber risks will affect their KSFs, and to make decisions based on these considerations (Figure 8).

For example, in the case of an e-commerce service, typical KSFs might be the ability of users to use the e-commerce website any time except during maintenance and the protection of customer information. Therefore, when a vulnerability in the software used in an e-commerce website is identified and reported, decisions can be made based on whether and to what extent those KSFs would be affected if and when the vulnerability is exploited.

If the company's products or services are sold or offered overseas, one KSF would be compliance (lack of conflict) with local regulations, and relevant data would need to be collected and analysed to determine the impact. In recent years, cyber security laws in China and privacy laws in various countries and regions have been enacted and enforced, requiring special attention.

Figure 7: In-house utilisation of threat intelligence

Q) How does your company utilise threat intelligence? (Select all that apply.)



[5] Ministry of Economy, Trade and Industry. 'Cyber Security Management Guidelines Ver 2.0'. (https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf)

2. Develop a cyber intelligence cycle that is appropriate for your organisation.

In recent years, the importance of open-source intelligence (OSINT) in threat intelligence activities has been repeatedly emphasised, and information can be collected from a variety of sources, including government agencies, industry organizations such as Information Sharing and Analysis Centers (ISACs), IT and security vendors, news and social media. As mentioned above, the survey results showed that about 80% of companies are collecting threat intelligence, but they are facing challenges in using it.

One of the reasons for this is that many companies have not fully developed their overall cyber intelligence activity cycle. This is especially the case when threat intelligence services are outsourced to specialised external vendors. When companies expect their external vendors to perform risk analysis on their behalf, they often lack the internal processes necessary to evaluate and analyse the suggestions and insights provided by the vendors. In our survey, many respondents also raised the following causes of challenges in using threat intelligence: 'Don't know how to use intelligence effectively' and 'The quality of the intelligence is not good enough for practical use' (Figure 9).

Figure 8: Setting indicators for evaluating cyber risks that could impact KSFs

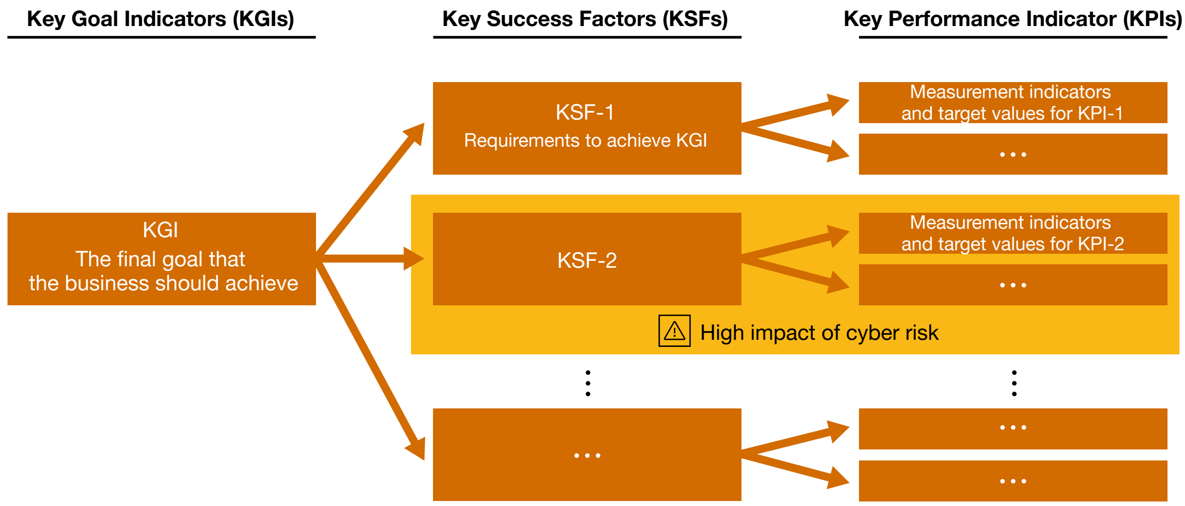
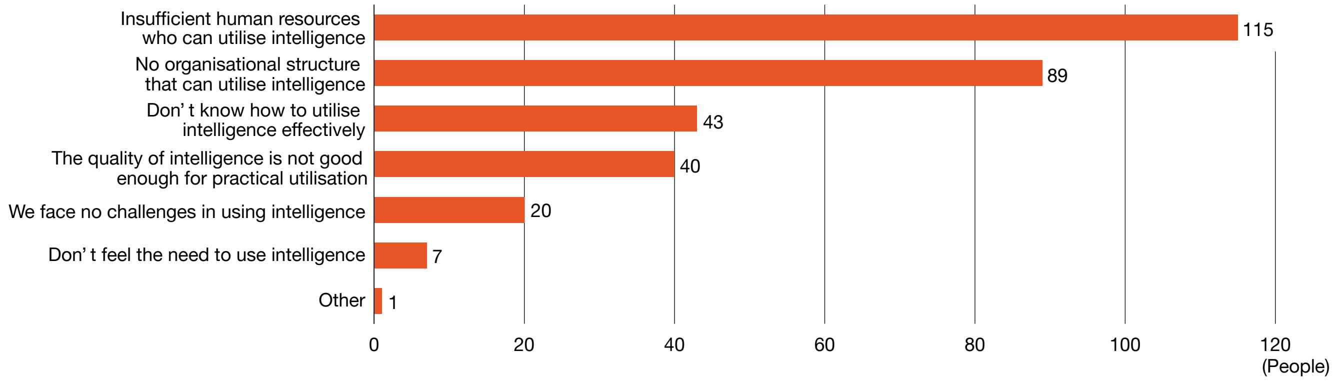

Key Goal Indicators (KGIs)
Key Success Factors (KSFs)
Key Performance Indicator (KPIs)
KSF-1
Requirements to achieve KGI
Measurement indicators and target values for KPI-1
...
KGI
The final goal that the business should achieve
KSF-2
Measurement indicators and target values for KPI-2
...
⚠ High impact of cyber risk
...
...
...

Figure 9: Challenges in utilising threat intelligence

Q) What challenges do you face in utilising threat intelligence, and if you face difficulties in utilising it, what are the reasons? (Select all that apply.)



The purpose of intelligence is to identify the impact of cyber risks on the KSFs of business operations and to support decision-making, which is not something that a third party can fully accomplish on behalf of the company. Therefore, it is essential for companies develop a process that is tailored to their own needs, while referring to basic frameworks such as the intelligence cycle,.

In general, intelligence activities are conducted by intelligence agencies based on requests from decision makers. They are carried out through a series of activity cycles such as policy formulation, collection, assessment, analysis, and distribution and feedback. In terms of corporate activities, policy formulation means setting the objective that intelligence collection is to achieve. This objective, as we previously explained, is the identification of cyber risks that could affect KSFs. To achieve this objective, it is also necessary to identify intelligence sources and evaluate the reliability of each source. Companies should then take the following actions in accordance with their newly formulated policy.

1. Collection
Collect intelligence.

2. Assessment
Assess the reliability of the intelligence itself based on its content, evidence, etc.

3. Analysis
Analyse the presence and degree of impact on KSFs and derive suggestions and opinions.

4. Distribution and feedback
Provide these suggestions and opinions to appropriate decision-makers and meeting bodies to make decisions.

3. Build an organisational structure in which business and IT divisions can collaborate.

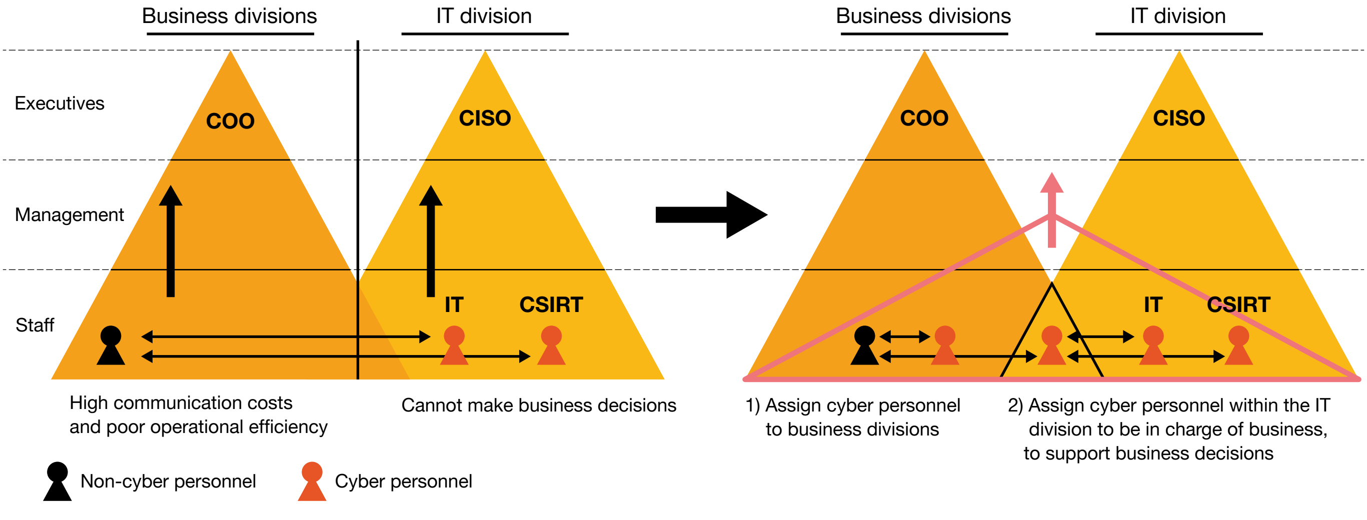
With the digitalisation of business, the number of KSFs affected by cyber risk continues to increase, and cyber-related issues are also becoming a larger part of decision-making. Therefore, it can be argued that cyber risks need to be treated as a management agenda, and that of course management, represented by the chief information security officer (CISO), should lead those response activities.

Intelligence-related activities in particular require the collection and analysis of a wide range of intelligence, not only from a technical perspective, but also from the perspectives of laws, regulations, and social and industrial trends such as industry guidelines. These activities naturally require a higher-level perspective. Therefore, it is important to identify the KSFs that are related to cyber risks as a matter of common understanding throughout the organisation, and to establish a process to extend KSFs to the relevant divisions in cases where comprehensive judgment is required, so that the intelligence that is collected and analysed can be put to effective use based on accurate knowledge of how to handle it.

In recent years, some companies have also established IT functions, including business-critical cybersecurity functions, within the relevant business divisions instead of in the corporate IT division. In such cases, each business division can operate their own internal cyber intelligence cycle to analyse the presence and impact of cyber risks on the business quickly and with high accuracy (Figure 10). At companies that, on the other hand, extend their cyber intelligence functions to existing CSIRT organizations, collaboration with business divisions is essential as the objective of cyber intelligence activities is to determine whether and to what degree KSFs are impacted.

Although the optimal structure will vary depending on the company, it is necessary in all cases to strategically build an organisational structure that allows IT and business divisions to collaborate, for example by assigning cyber personnel to the business divisions or assigning cyber personnel within the IT division to be in charge of specific businesses.

Figure 10: Example of effective corporate cyber staffing


Business divisions
IT division
Executives
Management
Staff
COO
CISO
IT
CSIRT
High communication costs and poor operational efficiency
Cannot make business decisions
Business divisions
IT division
COO
CISO
IT
CSIRT
1) Assign cyber personnel to business divisions
2) Assign cyber personnel within the IT division to be in charge of business, to support business decisions
Non-cyber personnel
Cyber personnel

Shuji Okuda
Director, Cybersecurity Division
Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry

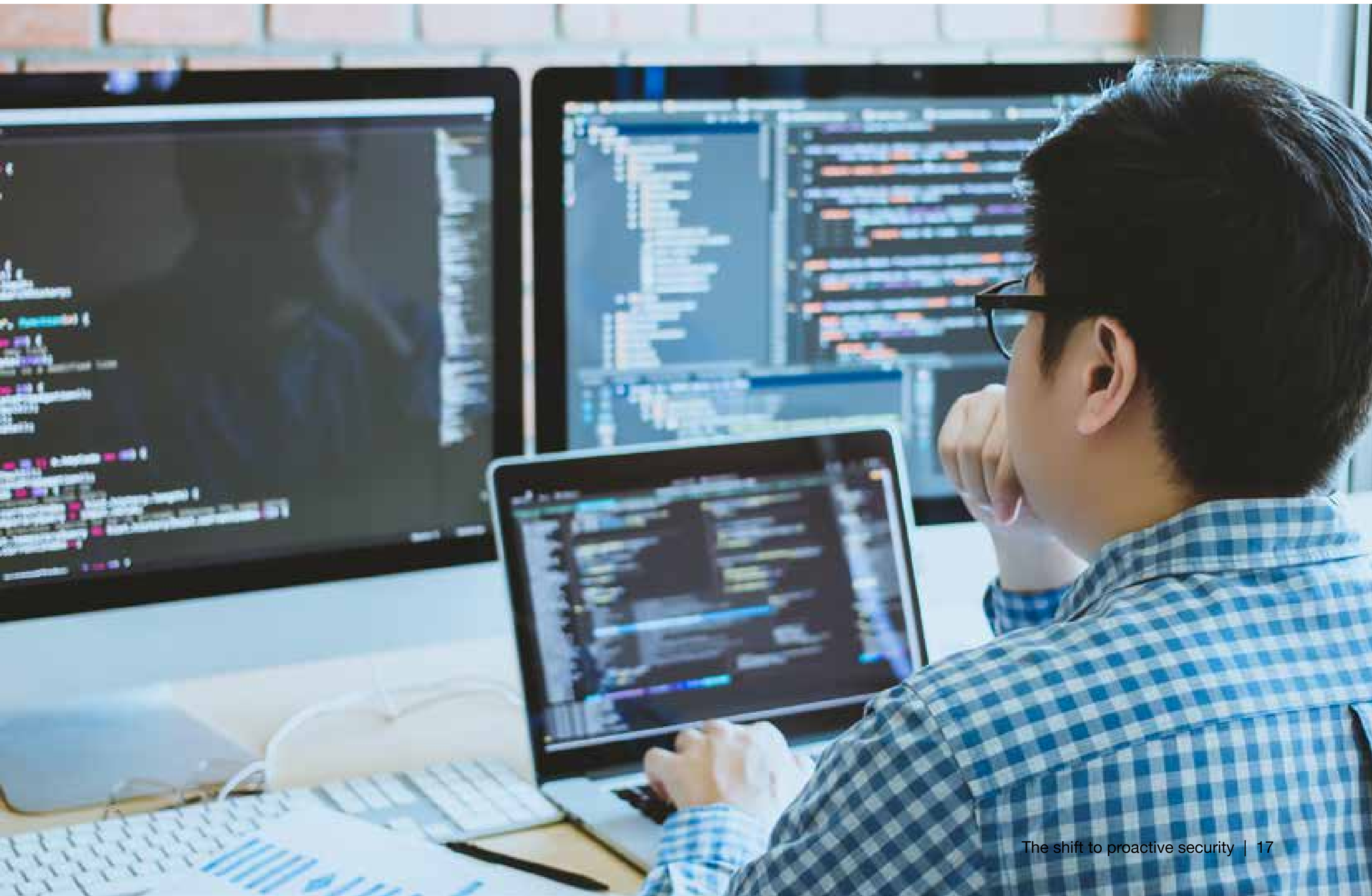
The number of cyberattacks is increasing every year, and in recent years, attacks that directly demand money, such as ransomware attacks, have become more prominent. If a company makes a mistake in responding to such attacks, it will not only suffer business losses but also lose social trust at the same time. Executives must recognise cybersecurity risks as business risks and promote appropriate cyber security measures.

However, there is a major issue here. Companies are not able to organise the cyber threat intelligence they have collected and are not able to use it as a valuable resource to generate the information that executives really want to know. A lot of information explains cyber threats from a technical viewpoint and provides warnings about measures to be taken. However, what executives want to know is not the methods and technical details of cyberattacks, but how much damage cyber threats may cause to their business continuity, credibility and intellectual property (IP), as well as how to respond.

It is important for executives to understand the degree of negative impact that current cyber threats have on their businesses and what IP is being targeted so that they can take concrete countermeasures. In order to do so, they need a system that provides information to help them make appropriate decisions.

The creation of such a system must be done through cooperation between government and industry. For example, if a security certification system is established overseas, it will naturally have an impact on Japanese companies. However, if Japan does not have a comparable certification system, it will be difficult to respond quickly. At a time when cyberattacks are becoming globalised, it is urgent for the government and industry to work together to design systems and establish guidelines.

The Ministry of Economy, Trade and Industry (METI) is responsible for promoting security measures in Japan by communicating closely with industry and supporting companies' voluntary efforts. We would like to create a field where it is easy for businesses to operate, and to promote an enhanced level of cybersecurity response in Japan.



Shinichi Yokohama
Chief Information Security Officer (CISO)
Senior Vice President, Security and Trust Office (STO)
NTT Corporation

There is a saying, 'strategy under uncertainty'. In the world of cybersecurity, threat intelligence is becoming more and more important, but even if we try to anticipate changes in the external environment, an element of uncertainty is involved. Nevertheless, in most cases the attacks we are exposed to are not completely unforeseeable. For example, if we carefully analyse cyberattacks in Western countries, we can, to a certain degree, formulate scenarios of the kind of threats that are likely to occur in Japan in the future. Collecting intelligence and taking countermeasures based on these scenarios are the first steps toward proactive security. However, the current situation is that people, including those in the business sector, are struggling to conduct these processes.

Technical intelligence includes important information that engineers in the field must address very quickly. Among the large volume of technical intelligence, such as software vulnerability information, that we receive every day, we prioritise and sort the information, and work with the business companies in our corporate group to take action. By reviewing the operational characteristics of each company and the response of the people in charge, we make various decisions. 'We should definitely respond to this threat.' 'Even if we report this threat to the people in charge, they will not be able to respond to it because they are very busy right now.' 'We should lower the priority of the threat.' And so on.

I believe that mutual understanding and trust between field managers and decision-makers is extremely important. The reason why I added the word 'trust' to the name of Security and Trust Office, which I have been leading since last year, is because I believe that it is impossible to make progress in security without relationships of trust between organisations as well as between individuals.

In addition to technical intelligence, we are also collecting non-technical intelligence. As NTT is shifting from a domestic business to an international business, we thought that we needed to understand how cyber security policies, trends, and regulations would change on a global level. We have therefore been keeping a close watch on global trends from the perspective of how laws and regulations, US federal government policies, and the EU General Data Protection Regulation (GDPR) will affect our business. A few years ago, I regularly travelled to the US to talk with members of public-private partnership councils and industry associations to monitor global security trends. During these activities, I became convinced that the issues occurring in the US would become worldwide trends, including in Europe, and would spread to Japan as well. I am also paying attention to how the world's leading telecom operators view non-technical intelligence. I have been exchanging information with CISOs of telecom operators in the US and Europe about their current issues and future policies. While I am learning about their approaches and perspectives, it is also important for me to determine our market view and the appropriate security levels (boundaries).

It has been six to seven years since I started monitoring global security trends and feeding them back to our own business. By gaining more experience, I have been able to identify vital points and use them to strengthen various measures, such as supply chain risk management. I also feel that I am gaining a sense of what will happen in the future and an ability to respond quickly.

In order to act in a proactive manner, we must be ready to anticipate what will be required in the future, based on both technical and non-technical intelligence. Raising the bar to a higher level will naturally require investment and resources, and this cannot be achieved without executive decision making. The determining factor will be the degree to which our leaders can lead.

Hisanori Matsuzawa
General Manager, Data Management Department
MS&AD Insurance Group Holdings, Inc.
General Manager, Data Management
Mitsui Sumitomo Insurance Co., Ltd.

In the past, the main purpose of cyberattacks targeting non-life insurance businesses was to steal personal information and sell that information on illegal websites to gain money. Today, however, the price of personal information has plummeted, and businesses are strengthening their measures against information leaks. Currently, ransomware attacks are on the rise. As attack methods are constantly changing, executives must understand the attackers' aims, determine what the threat is to their business, and make the final decision on budget allocation and countermeasures. Security personnel need to provide information that enables executives to understand the differences in attack targets and changes in threat trends, and to make decisions on how much and where to allocate the budget and what countermeasures to take.

One of the features of MS&AD Holdings' security measures is the existence of our supply chain, which includes affiliated businesses, more than 100 overseas offices, subcontractors and agencies. The security risks we face differ depending on the type of business, business conditions, and scale of each agency or location. Therefore, it is not practical to require one-size-fits-all security measures for the entire supply chain. Even in Japan, while it is sufficient to promote governance based on the FSA’s guidelines for affiliated businesses, insurance agencies are not necessarily specialised businesses and often operate other businesses as well, so we need to consider guidelines tailored to each industry. Overseas offices located in North America, Europe, Asia need to be adapted to the laws, regulations and culture of each country. The scope of protection is very wide, including cloud providers and other outsourced businesses. Therefore, must detect any risks in our business, including the supply chain, on a daily basis and develop countermeasures.

In fact, even as we report at our management meetings on the latest status of group governance, including our overseas offices and agencies, the number of new attacks is increasing. Since attacks take place almost every day, I believe that there is little point in reporting on what we were able to do in the past. Therefore, we are working to create a system that allows local staff to understand their own cyber risks and take security measures independently. Specifically, we are aiming to enable our people to autonomously consider the necessary countermeasures for each location based on the types of threats that are on the rise, examine their plans and secure the resources to implement the necessary measures. We are also thinking of creating a system to share best practices at each site and planning a centralised global operation centre for group synergy. If local staff can take actions according to the risk level of each site, we will be able to increase resilience and achieve wide-area protection.

While we consider cyber risks from the aspect of dealing with our own business, our mission is to correctly recognise risks and make them known to society. Going forward, we will continue to help businesses appropriately assess risks and promote risk countermeasures.

3. The reality of Japanese corporate security in 2021

Corporate outlook on cyber security
from the 2021 Cyber IQ Survey findings

Security investment will increase with a focus on response and recovery.

Currently, 31.4% of the respondents reported investing 10% or more of their IT-related budget in information security, but the number of respondents who plan to be investing 10% or more three years from now increases to 41.6%. Analysis of the results by respondent shows that about 40% of the total respondents intend to increase their information security budget. And a significant number of those respondents are planning to increase their budget by about 10% (answering '10% to 20%' for their current budget and '20% to 30%' for their budget in three years). In terms of specific areas, as mentioned in the main report, investments related to response and recovery are expected to increase (Figure 11).

Cyber insurance enrolment rates will be boosted by compensation for incident response costs.

According to the survey, 75% of respondents do not have cyber insurance at present, but the number of respondents who do not plan to enrol in cyber insurance within the next three years decreases to about 42%. Regarding the coverage that businesses that are considering enrolling in or expanding their cyber insurance in the future expect to have, the top responses were 'Crisis management', 'Loss or theft of personal information', 'Lawsuits arising from security-related incidents', 'Incident response', and 'Incident recovery'. This suggests that businesses want to compensate for losses related to the occurrence of incidents (Figure 12).

Figure 11: Comparison of current information security budgets and planned information security budgets three years from now as a percentage of IT-related budgets

Q) How much of your business's information technology-related budget was allocated to information security in this fiscal year? How much do you think will be allocated to information security three years from now? (Choose only one response for each.)

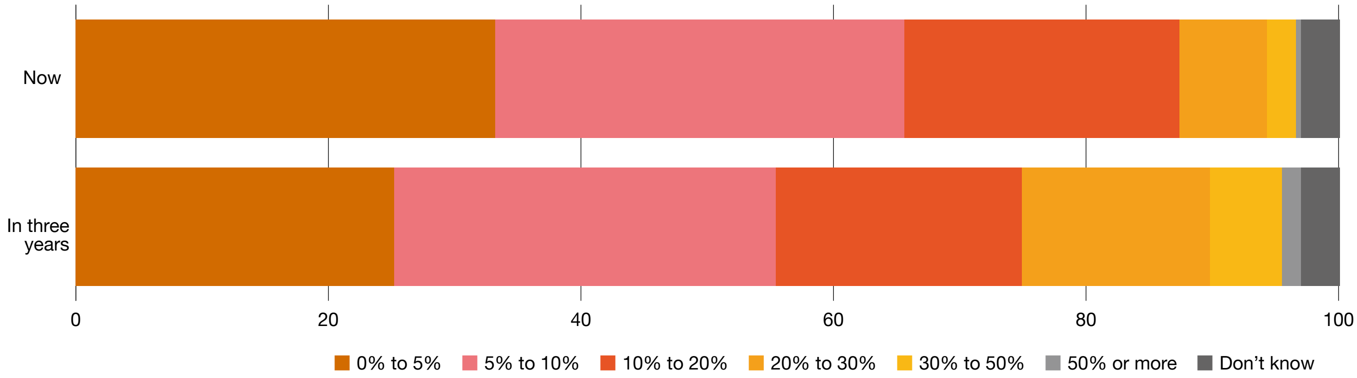
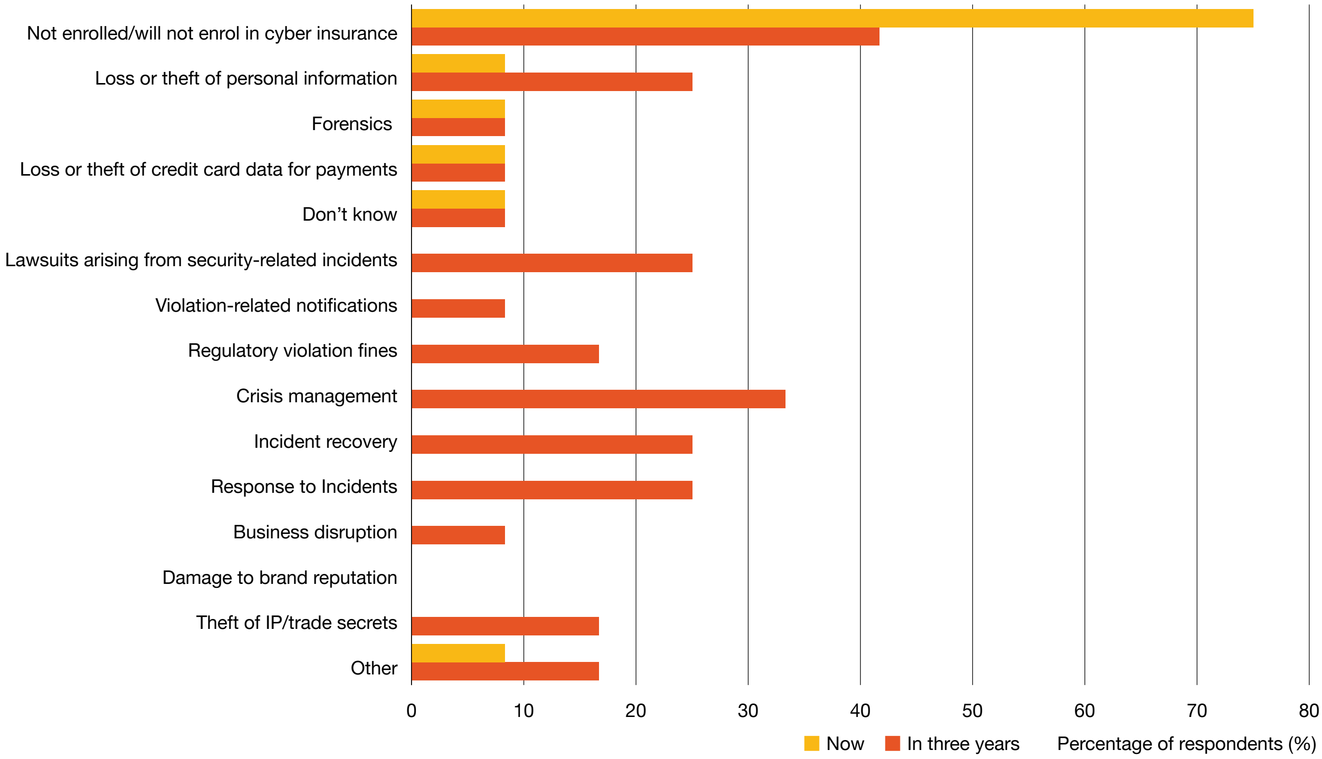


Figure 12: Coverage details of companies' current cyber insurance enrolment and planned enrolment three years from now

Q) If you currently have cyber insurance, what kind of losses are covered? If you plan to enrol in cyber insurance or expand your current coverage in the next three years, what kind of losses do you expect to be covered? (Select all that apply.)



Companies are aiming for centralised security governance.

About 40% of all respondents answered that they didn't have any overseas offices, and about 30%, or half of the remaining 60%, answered that their head office proactively oversees the security measures of overseas offices. The number of respondents who answered that they will still be leaving security measures up to their overseas offices three years from now shows a slight decrease in comparison with those that are currently doing so, and the number of respondents who answered that the head office will be controlling or monitoring security measures three years from now was greater than those currently doing so. This indicates a trend for the head office to gradually become more engaged in the security control of overseas offices in the future (Figure 13).

Development of incident response plans that involve contractors are in progress.

Currently, many companies are trying to control the security of external collaborators and contractors by signing security agreements with stakeholders. Although this measure clarifies the scope of responsibility of both the company and the stakeholder, many companies now recognise that this issue cannot be addressed simply by defining responsibilities, as the outsourcer must respond to any incidents at their contractors, and may suffer a loss of credibility in the market. For this reason, we expect that an increasing number of businesses will implement more in-depth controls for stakeholders, such as more effective management of stakeholders through the establishment of an incident response system that includes stakeholders, indicated by the number of respondents who answered 'Developing an incident response plan that involves stakeholders,' and through risk assessment of stakeholders. On the other hand, about 20% of all respondents answered that they don't know what kind of security measures they are taking for stakeholders now or which measures they plan to take over the next three years, indicating that they have not yet found effective security controls and measures for external collaborators and contractors (Figure 14).

Figure 13: Security control methods for overseas offices that companies have implemented (and are considering implementing over the next three years)

Q) If you have overseas offices, how do you implement security controls for them? And how do you plan to implement security controls for them in the next three years? (Select only one response for each.)

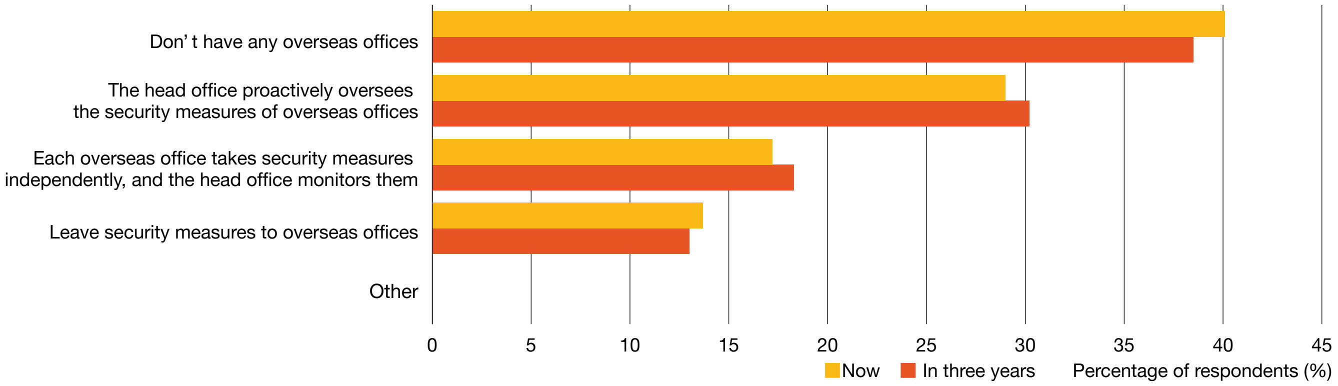
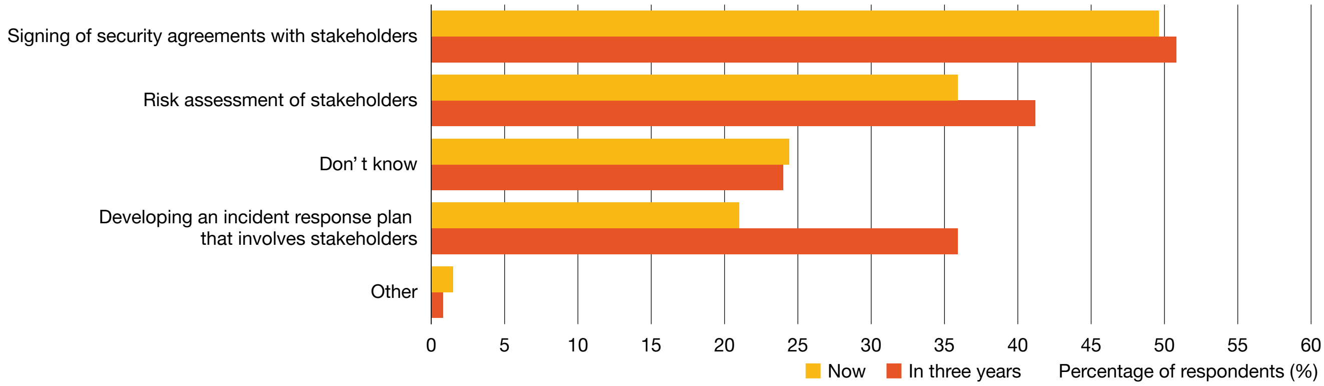


Figure 14: Security measures which companies have implemented for external stakeholders (and are considering implementing over the next three years)

Q) Please select the security measures you have implemented for your external stakeholders (collaborators, contractors, etc.) and which you are considering implementing over the next three years. (Select all that apply.)



Current use of cloud security functions is limited but will be accelerated by the shift to zero-trust architecture.

Although only about 40% of respondents currently store confidential data on cloud services, the total percentage of companies that plan to do so or are considering doing so in the future is about 70%. We expect, therefore, that the majority of mainstream business and service provision will be centred on cloud environments, which offer significant advantages in terms of operational management and business efficiency, rather than on-premises environments. In addition, many cloud security measures currently in place are limited to access control and security screening at the time of cloud use, indicating that few businesses are focusing on cloud security measures. However, the number of respondents who said that they will be taking security measures such as anomaly detection and policy violation detection over the next three years increases remarkably, indicating that more companies will be promoting cloud security measures in the future, in response to the shift to zero-trust architecture (Figure 15).

Companies are facing a security personnel shortage and examining prospects for solutions.

About 80% of all respondents cited a shortage of security personnel, which highlights the current talent shortage facing businesses. Many companies responded that the best way to solve this issue was to take measures to increase their security personnel, such as training existing personnel (34.5%), outsourcing (32.0%), and hiring new personnel (25.5%). On the other hand, only 6.5% of the respondents answered that the best way is to reduce security tasks through automation, etc., indicating that few businesses expect automation to solve the security personnel shortage. However, we can also expect the importance of automating security operations to increase in the future, as more than 90% of the respondents answered that they are working on automating some security operations over the next three years (Figure 16).

Figure 15: Security measures that companies have implemented (and are considering implementing over the next three years) with regard to the use of cloud services

Q) What security measures related to cloud services are you taking now, and which are considering taking within the next three years? (Select all that apply for each.)

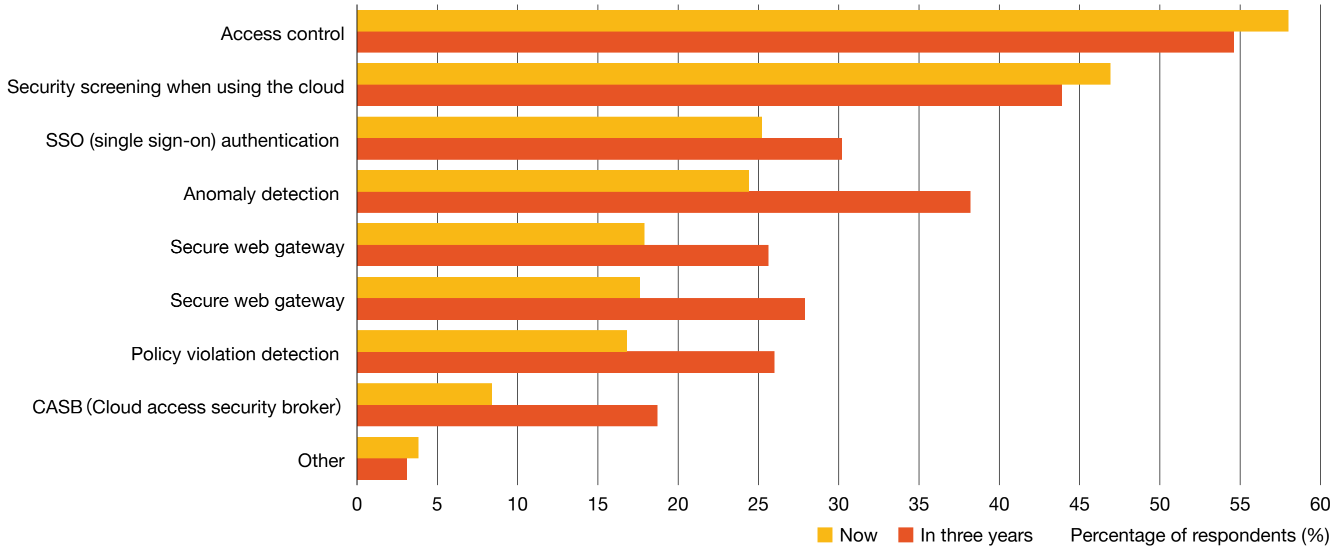
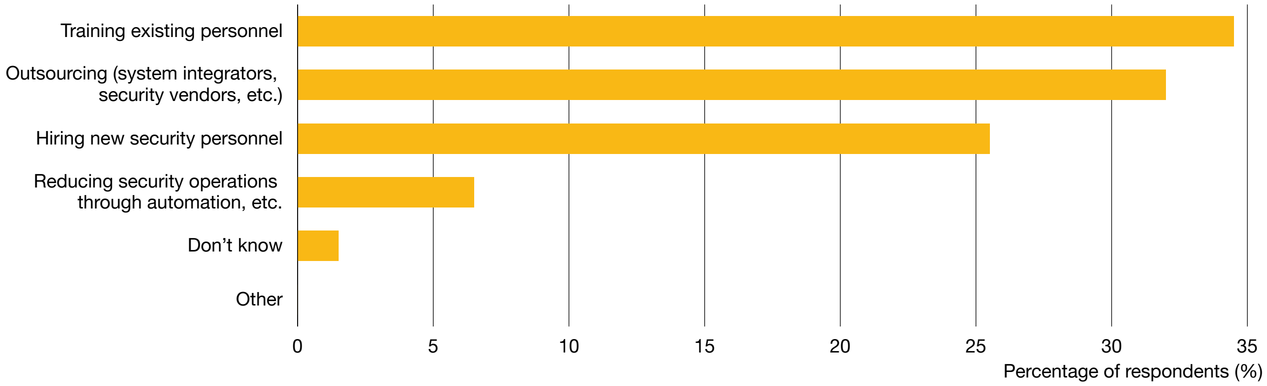


Figure 16: How companies think they can solve the security personnel shortage

Q) What do you think is the best way to solve the problem of the security personnel shortage? (Select only one response.)



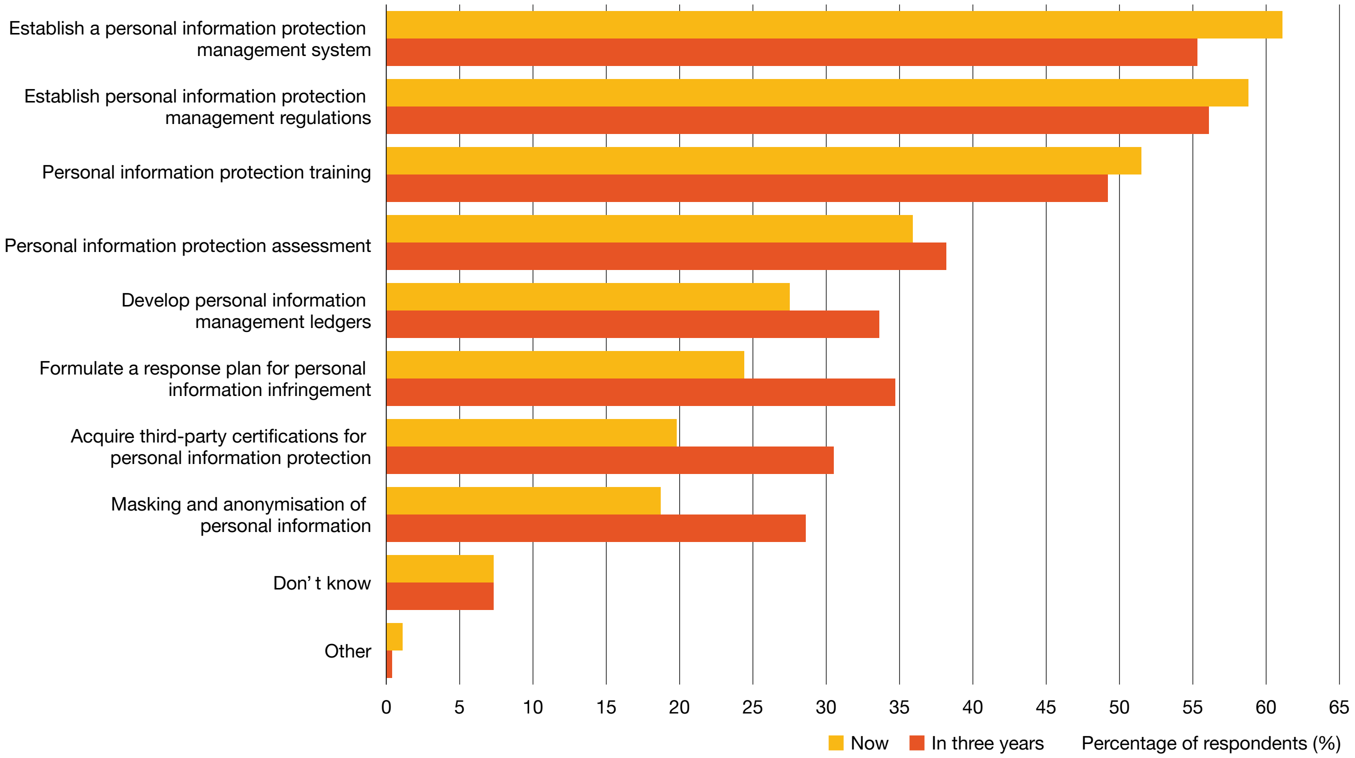
Concern about privacy protection is on the rise due to the enforcement and revision of laws and regulations in various countries.

In recent years, incidents involving personal information leaks have been occurring on a daily basis, and consumers are becoming increasingly concerned about the issue. In addition, privacy laws are being enforced and revised overseas, and many companies are under pressure to respond to these laws. We therefore believe that the increase in the number of respondents who plan to work on acquiring third-party certification for personal information protection over the next three years is due to a need to objectively understand the maturity of their own personal information protection measures and to demonstrate to consumers the safety of their services.

In addition, the enforcement and revision of laws and regulations both in Japan and abroad have resulted in stricter requirements for businesses. To comply with these requirements, a significant number of respondents answered that they plan to introduce new measures over the next three years, including the development of personal information management ledgers, the formulation of response plans for personal information infringement, and acquisition of third-party certifications for personal information protection (Figure 17).

Figure 17: Personal information protection measures that companies have implemented (and are considering implementing over the next three years)

Q) Please select the personal information protection measures you currently have in place, and those that you plan to implement over the next three years. (Select all that apply.)



Conclusion

Over the course of the COVID-19 pandemic, cyberattack methods have evolved in line with the spread of cloud computing among businesses, and an increasing number of cyberattacks have impacted business continuity. The transformation of cyberattacks into a kind of ‘industrial enterprise’ where cyberattack know-how can be sold and purchased without advanced hacking-related knowledge, allowing cyberattacks to be carried out in a relatively easy manner, has unfortunately become a characteristic of our time.

The ever-changing cybersecurity landscape and increasingly sophisticated cyber threats are forcing companies to change their attitudes toward cybersecurity. It has now become necessary to leverage cyber intelligence to ascertain the latest threat trends, determine which countermeasures to focus on, and make dynamic adjustments on a daily basis.

Now is the time to consider making the shift to proactive security. We hope that the specific actions described in this paper will help you take a step toward a major change in your security measures.

Contact us

PwC Japan Group
www.pwc.com/jp/ja/contact.html

Supervisors

Kazuhiro Hayashi
Partner, PwC Consulting, LLC

Mitsuhiko Maruyama
Partner, PwC Consulting, LLC

Authors

Junichi Murakami
Director, PwC Consulting LLC

Ryosuke Fuchi
Manager, PwC Consulting LLC

Misato Miyauchi
Manager, PwC Consulting LLC

Tiancheng Zhan
Senior Associate, PwC Consulting LLC

www.pwc.com/jp

The PwC Japan Group is a collective name for the member firms of the PwC global network in Japan and their affiliates, including PricewaterhouseCoopers Aarata LLC, PricewaterhouseCoopers Kyoto, PwC Consulting LLC, PwC Advisory LLC, PwC Tax Japan, and PwC Legal Japan. Each firm within the PwC Japan Group conducts its business as a separate, independent business entity.

In response to our clients' increasingly complex and diverse corporate management issues, the PwC Japan Group has put in place a system that consolidates our knowledge in the fields of auditing and assurance, consulting, deal advisory, tax and legal services, and encourages organic collaboration among our professionals in each field. As a professional services network with approximately 9,400 certified public accountants, tax accountants, lawyers and other professional staff, we strive to provide services that more accurately address our clients' needs.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 156 countries with more than 295,000 people who are committed to delivering quality in assurance, advisory and tax services.

The electronic version can be downloaded from: www.pwc.com/jp/en/knowledge.html
Issued April 2022.   Control number: I202201-05

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.