Stakeholder Survey 2019
An In-depth Study on Security

Organizer：Taiwan Network Information Center

Implementer：InsightXplorer Ltd.

Contents

Chapter I. Research Summary 2
I. Research Background 2
II. Research Goal 2
III. Research Methodology Overview 4
IV. Research Process 5
V. Survey Methodology Overview 5
Chapter II. Profile of Taiwanese Enterprises' Information System Usage 7
I Executive Summary 7
II Industry Characteristics 8
III Business Size 10
Chapter III. IT System Usage and Maintenance 15
I The larger the business size, the more often it accesses personal information 15
II Outsourced Security Tasks 16
III Security Service Purchase/Rental/Subscription 18
IV Self-Assessment on Security Protection and Requirements Details 20
V Security Requirement Details 22
Chapter IV. Security Incidents and Awareness Planning 25
I Cyber Attacks and Damages 25
II Security Incident Reporting and Solution Assistance 26
III Security Concerns 28
IV Enterprise Security Planning 29
V Attitude towards Security Planning 31
Chapter V. TWCERT/CC Recognition and Interaction 34

I Awareness and Interaction 34
II Awareness/Interaction/Security Demand 34
III Overall Satisfaction/Sentiment towards Service Value 35
IV Building Reciprocal Relationships and Future Development of Security Reporting.....37
V Future Directions of Interaction.....38
VI Incentives to Seek Assistance 40
VII Suggestion and Expectation.....41
Chapter VI. Recommendations 44
Goal: short-term: Promoting Incident Coordination and Handling
Long-term: Establishing Preventive and Protective Mechanism....44
I To Continue Providing Security Consultation Services/Sharing Info/Identify Service Req. from the Surface Downward 44
II To Provide Diverse Education/Training from Security Literacy for Employees to Nationwide Security Education 46
III With Half of the Enterprises at Risks, it is Imperative to Understand the Req. and Create Industry Guidelines 49
IV Legal Awareness in Security Training and Specific Assistive Prevention Service Plans.....50

Chapter I. Research Summary

Chapter I. Research Summary

I. Research Background

In 2018, Taiwan's National Security Council announced its first cyber security strategic report in which highlights the importance and value of cyber security and illustrates the concept/goal of 'Cyber Security Equals to National Security.' According to 2019 iThome Comprehensive Security Report, up to 70% of the enterprises have suffered at least one security attack in the past year. The report also finds the gradually increasing demand of security talents and the need to engage more security resources. All organizations, whether in public or private sector, have demonstrated high level of concerns and paid close attention to this topic.

Since 2019, TWNIC has taken over the operation of TWCERT/CC and started to work on its position as a service provider and offer a wide range of comprehensive services. Based on the findings of Stakeholder Survey 2019 : An In-depth Study on Security, this report investigates the security requirements of private enterprises in Taiwan to get a full picture of reporting requirements and set up a trust mechanism. The goal is not only to achieve effective security reporting, but also for TWCERT/CC to better perform its role in bridging the public and private sector, develop services for and initiate collaboration with key stakeholders, as well as strengthen the links on enterprise cyber-security.

II. Research Goal

To be cognizant of Taiwanese enterprises' security requirements and their opinions regarding incident reporting, this study has performed

quantitative and qualitative researches concurrently to obtain a holistic picture of the general IT environments before deep diving into specific topics. The study will take 'trust building' as its research dimensions. For instance, it examines how Taiwanese companies use their IT systems, their security capabilities and foundations, security reporting requirements, and reporting methods. It is expected that the following goals can be achieved:

i. Through quantitative and qualitative researches, obtain the profile of how Taiwanese enterprises use information systems and identified the enterprise requirements for holistic IT security reporting.
ii. Based on the survey results, a focus group session was held with security experts, business owners and alliance members to discuss about future service development and collaboration with primary stakeholders
iii. To understand Taiwanese enterprises' requirements for security reporting and how to establish the trust mechanism so as to achieve the goal of effective security reporting

III. Research Methodology Overview

One-on-one In-depth Interviews	
Interviewees	Head of IT dept. or person in charge of IT management in the target industry
Number of Interviewees	6
Interview duration and time	The interviews were conducted in April and Aug 2020, one hour per session
Interview Location	Phone interview, video conference, interviewee's office, or other convenient locations
key interviewer	IX team

Internet Survey Methodology	
Target	Supervisors or employees who have Internet-connected systems*[1] and the authorization to maintain or make decisions for the systems in Taiwanese enterprises.
Target Population	Taiwanese enterprises with Internet-connected systems - hospitality and manufacturing
Survey Duration	Pretest: May 22 - May 25 2020 Formal Test: June 1 - June 23 2020
Number of Samples	The minimum sample size is 529, with 95% of the confidence level and ±4.26% of the sampling errors.
Sampling Design	Purposive sampling and random sampling (Increase the exposure of questionnaires via newsletters and sample repositories and then select qualified interviewees from questionnaire respondents)

[1] IT systems in this report refer to the enterprise systems built to consolidate software, hardware and remote communication networks and used to collect, create, make and distribute accessible data. They can be professional computer systems with specific functionalities, ERP systems or AI-enabled applications.

IV. Research Process

- Questionnaire Preparation
- IX member database, IX Panel, cloud sample repositories of business partners, list of hotel businesses online (5000 records) iThome Weekly subscribers
- Result of Convergence Analysis

V. Survey Methodology Overview

In-depth interviews

- Survey conducted: 2020/04/28 - 2020/08/14

Interview date	Company/organizational unit	Company/organization description	Job title
April 28, 2020	A subsidiary of a large TW tech manufacturer	with 200+ employees, mainly producing computers, cell phones, and their parts	CTO
April 29, 2020	A TW electronics manufacturer	with 200+ employees, scope of business includes providing hardware and software to other SMEs	CTO
Aug 10, 2020	A TW electronics manufacturer	This global electronic component provider is a listed company in Taiwan, with 50+ employees based locally and more than 1000 in the group company.	Assistant manager
Aug 10, 2020	A TW manufacturer	Listed company in Taiwan with 500+ employees	Director
Aug 11, 2020	A TW hospitality business	Taiwanese hotel chain with 8 locations	Specialist
Aug 14, 2020	A TW industry manufacturer	A Taiwanese company with more than 5 decades of manufacturing experiences, selling products overseas and domestically, with 50+ employees	Section chief

Online survey

- Pretest: 2020/05/22 - 2020/05/25
- Formal test: 2020/06/01 - 2020/06/23

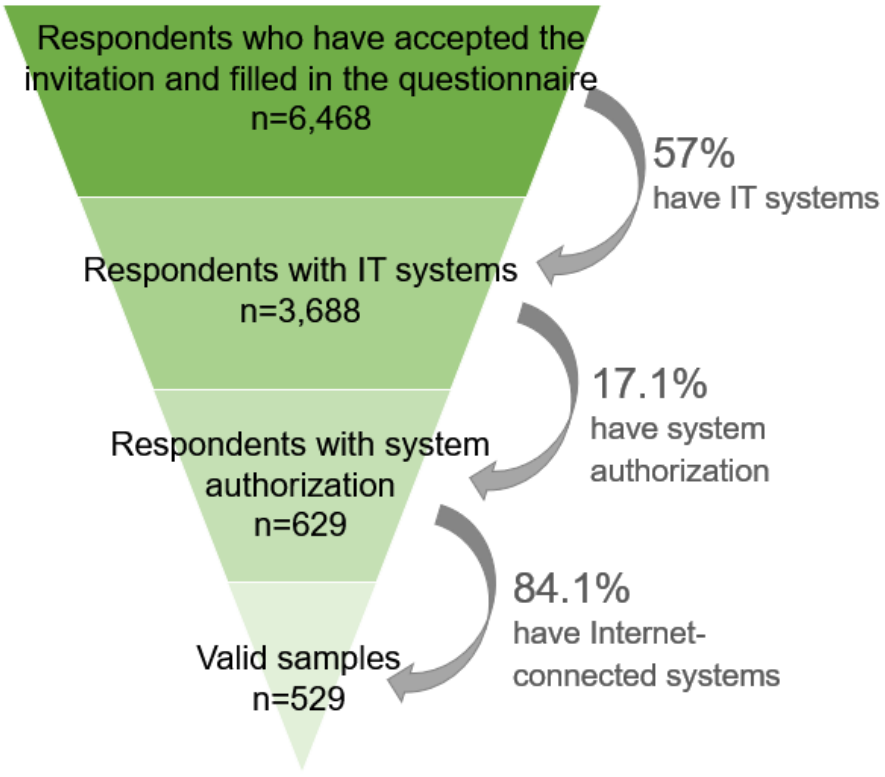
Industry type \ Source of samples	Total of valid samples (A+B)	IX member database and cloud sample repositories (including hotel owners) Number of valid samples (A)	iThome Weekly Number of valid samples (B)
Total (a+b+c)	529	393	136
Manufacturing (a)	185	135	50
Hospitality (b)	150	147	3
Other industries (c)	194	111	89

Chapter II. Profile of Taiwanese Enterprises' Information System Usage

Chapter II. Profile of Taiwanese Enterprises' Information System Usage

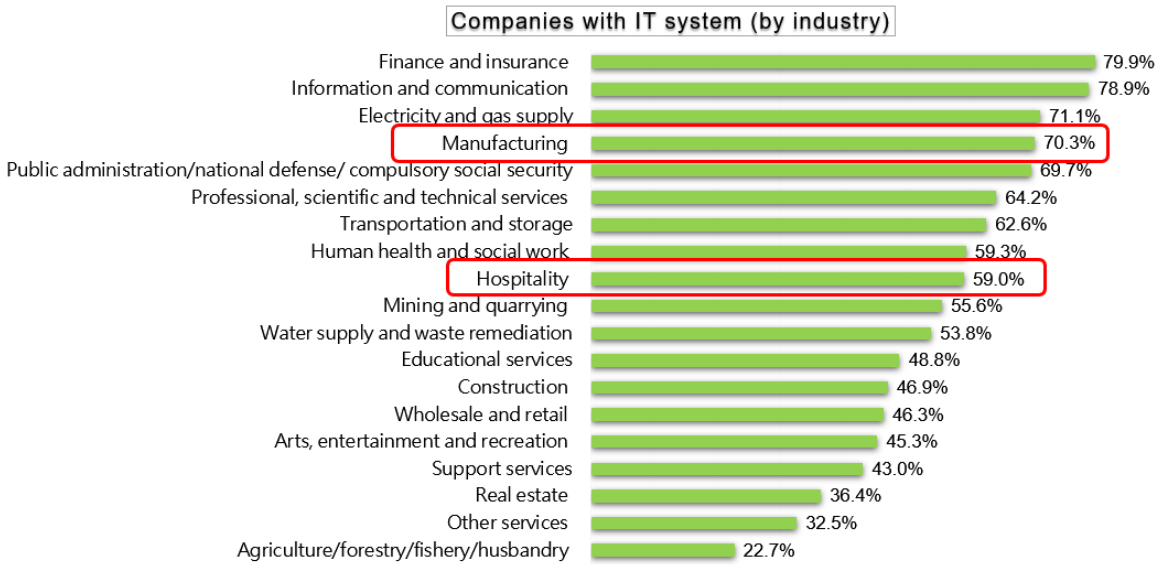
I Executive Summary

Out of 6,468 records, 57% of the respondents work at companies with IT systems.Out of 3,688 records, 17.1% of them have IT system authorization.Out of 629 records, 84.1% of them have Internet-connected systems.Filtered with the above criteria, 529 records have been selected as valid samples.



Source: This report (2020)

This research has collected 529 valid responses. The research mainly focuses on the proportion of companies with IT systems by industry and it finds 70.3% in manufacturing and 59% in hospitality businesses.

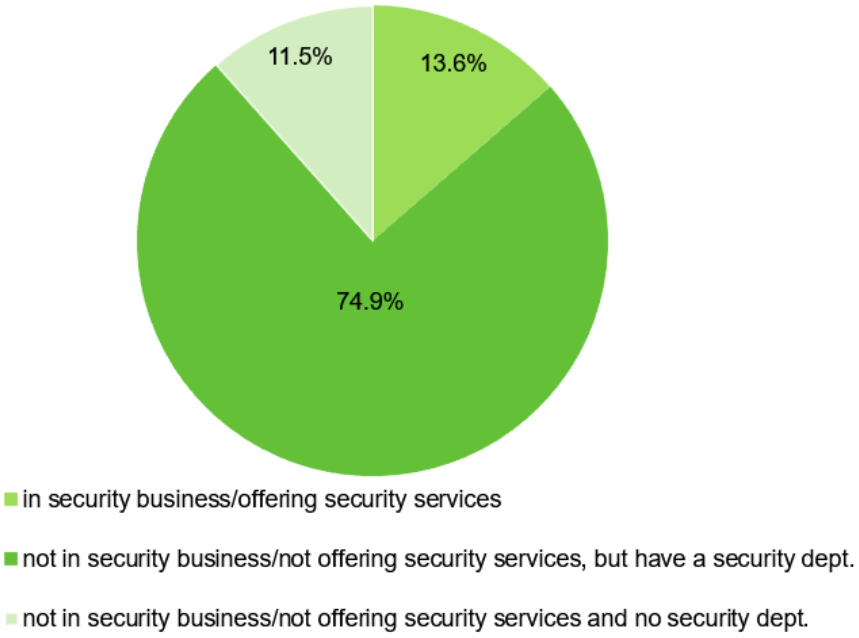


single choice, n=529

Source: This report (2020)

II Industry Characteristics

Based on our findings, 74.9% of the companies say they have a designated department in charge of IT security even though IT security is not their primary business/services. Among them, hospitality businesses with IT department staffed with 6-10 people make up a rather big proportion.



Source: This report (2020)

For industries categorized as 'other industries,' please see details on the left. Among the ones in 'other industries,' information and communication (7.8%) has the highest percentage, followed by wholesale and retail (5.1%) and all the rest account for less than 4%.

Industry	Valid Samples n=529	
Mfg.	185	35.0%
Hospitality	150	28.4%
Other	194	36.6%

	Valid Samples	
Agri/forestry/fishery/husbandry	5	0.9%
Mining and quarrying	1	0.2%
Electricity and gas supply	5	0.9%
Water supply & waste remediation	0	0.0%
Construction	12	2.3
Wholesale and retail	27	5.1%
Transportation and storage	3	0.6%
Information and communication	41	7.8%
Finance and insurance	12	2.3
Real estate	4	0.8%
Profl/scientific/technical services	13	2.5%
Support services	6	1.1
Public administration and defense; compulsory social security	8	1.5%
Education	20	3.8%
Human health and social work	14	2.6%
Arts, entertainment and recreation	7	1.3
Other services	11	2.1

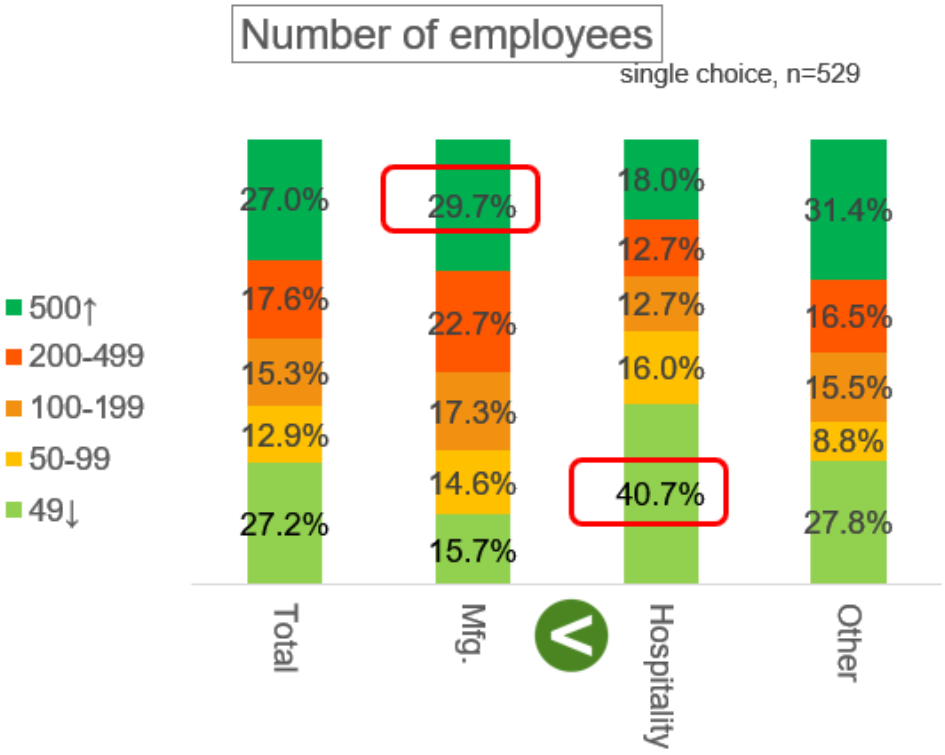
Source: This report (2020)

III Business Size

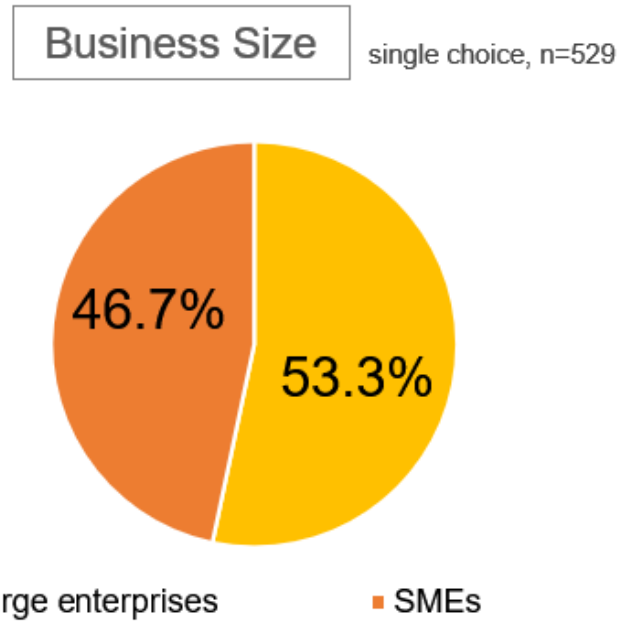
27.2% of the enterprises are staffed with 'less than 49 employees.' 40% of the hospitality businesses have workforce under 49 people while only 15% of manufacturers have the same staff size. The stats show manufacturing has larger workforce than hospitality.

For companies we surveyed in this report, 46.7% are large enterprises*, while 53.3% are SMEs[2]. In subsequent cross analysis, the difference in business size will be used for further study.

[2] According to Standards for Identifying SME stipulated in SME Development Statute, SMEs refer to enterprises which hire fewer than 200 regular employees in manufacturing, construction, mining and quarrying industries or businesses which hire fewer than 100 regular employees in the industries other than the aforementioned ones.



Source: This report (2020)

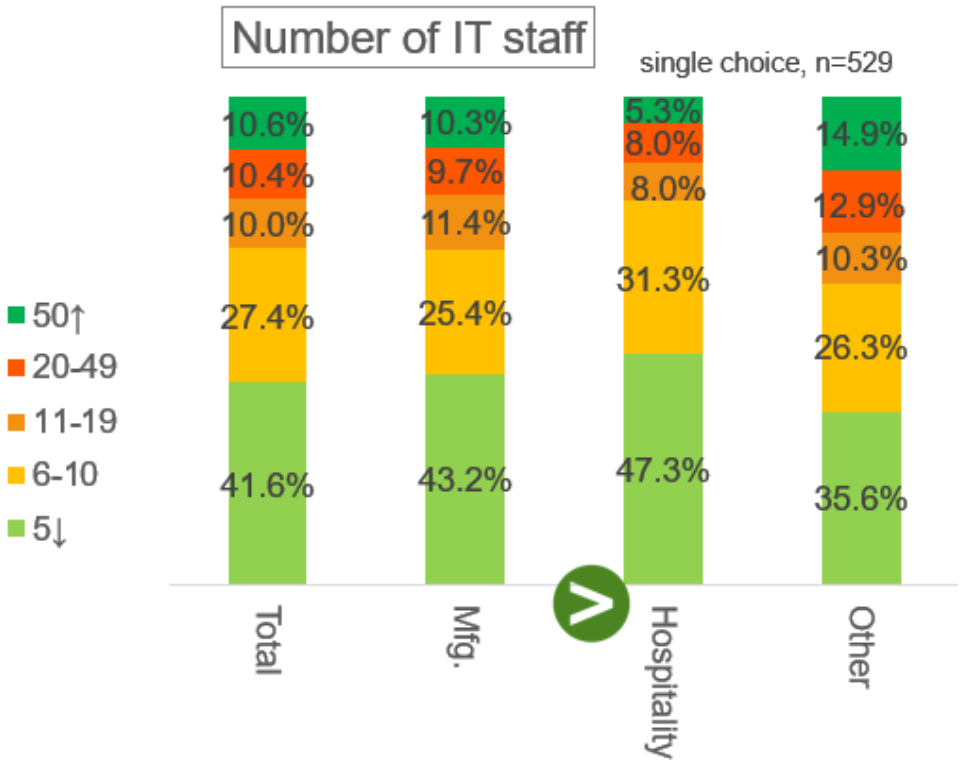


* According to Standards for Identifying SME stipulated in SME Development Statute, SMEs refer to enterprises which hire fewer than 200 regular employees in manufacturing, construction, mining and quarrying industries or businesses which hire fewer than 100 regular employees in the industries other than the aforementioned ones. ◦

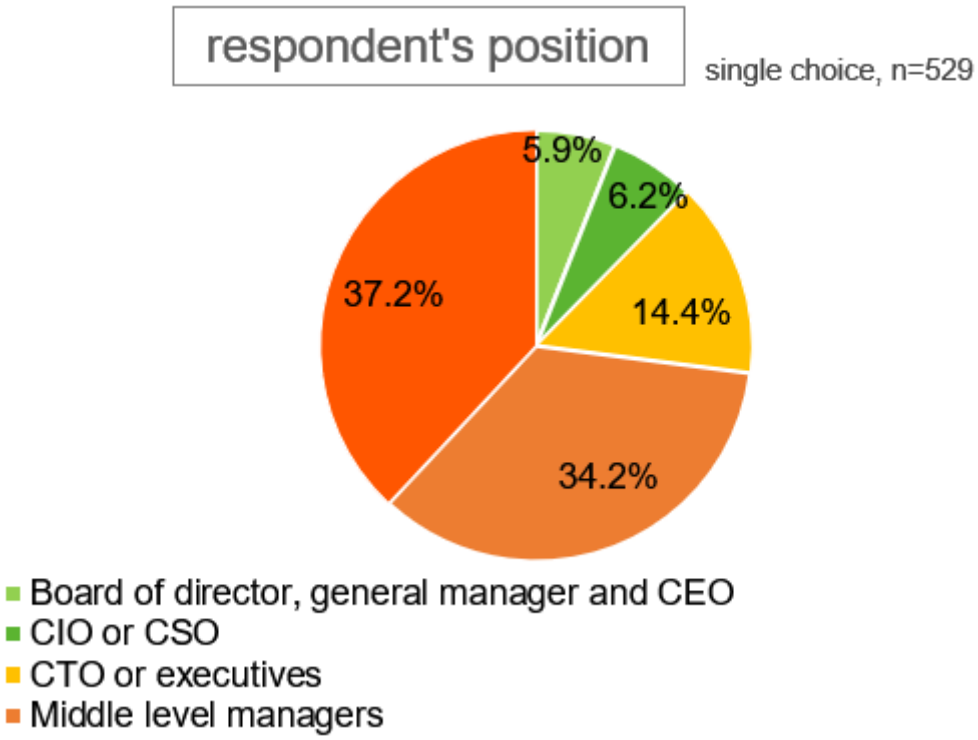
Source: This report (2020)

Pertaining to IT department staff numbers, the survey shows companies with 'less than 5' IT staff accounts for 41.6%, followed by '6-10' with 27.4%. Number of IT staff members is proportional to the total number of employees. This means large enterprises have relatively sufficient human resources to oversee IT system. Among them, businesses in manufacturing have more IT staff than businesses in hospitality.

Regarding the respondents' job positions, 37.2% are 'general technicians,' 34.2% are 'middle level managers' and around 15% are 'technical officers or executives.' As for top level management such as 'chief information officer and chief security officer' or ' board of director, general manager and CEO,' they each account for around 6%.



Source: This report (2020)



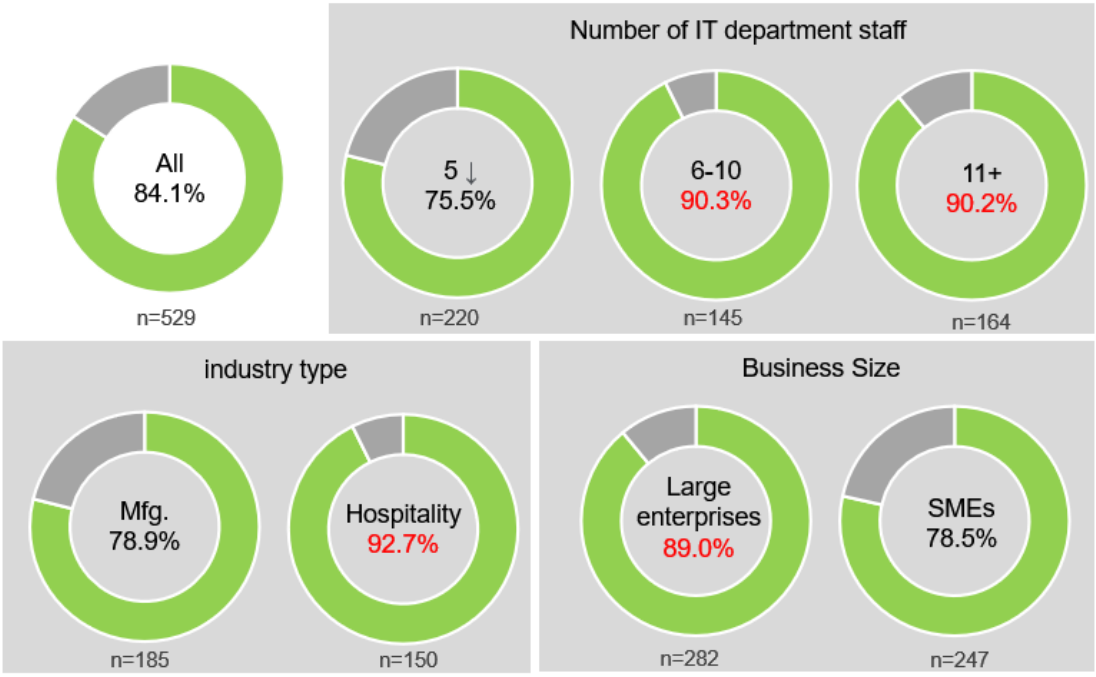
Source: This report (2020)

Chapter III. IT System Usage and Maintenance

Chapter III. IT System Usage and Maintenance

I The larger the business size, the more often it accesses personal information

84.1% of the responses say their companies have personal information stored in the IT system. Businesses in hospitality whose type is large enterprise and whose IT department is staffed with 6+ employees have significantly higher percentage.

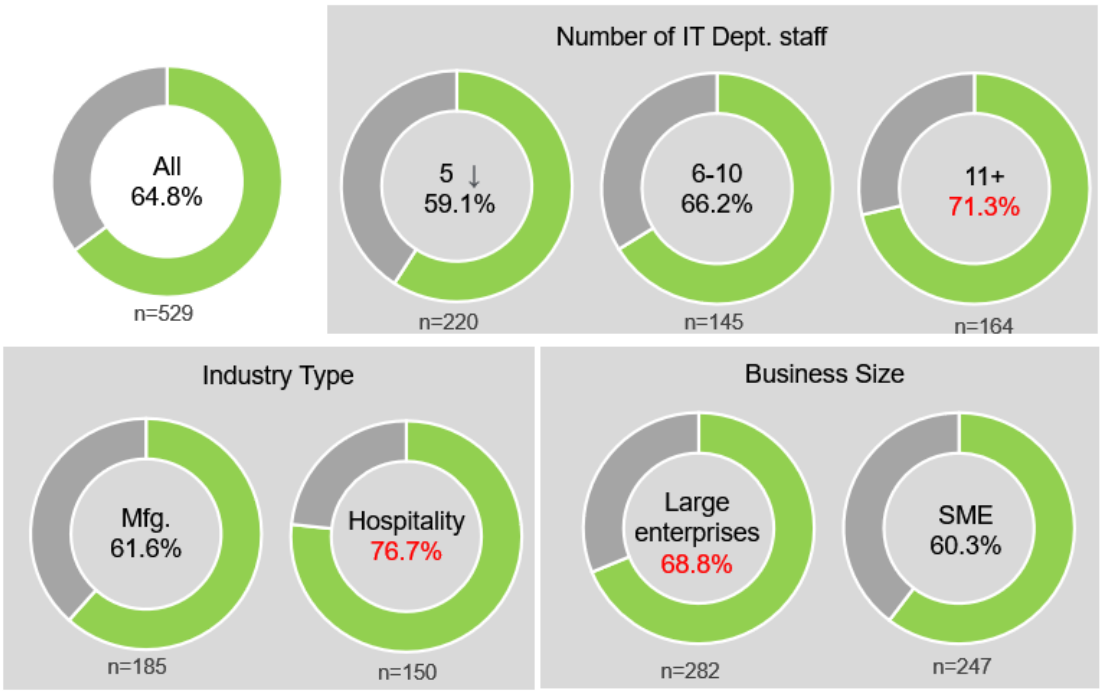


single choice

Source: This report (2020)

64.8% of systems are using vendor services for maintenance. Businesses in hospitality whose type is large enterprise and whose IT department is staffed with 11+ employees have significantly higher percentage.

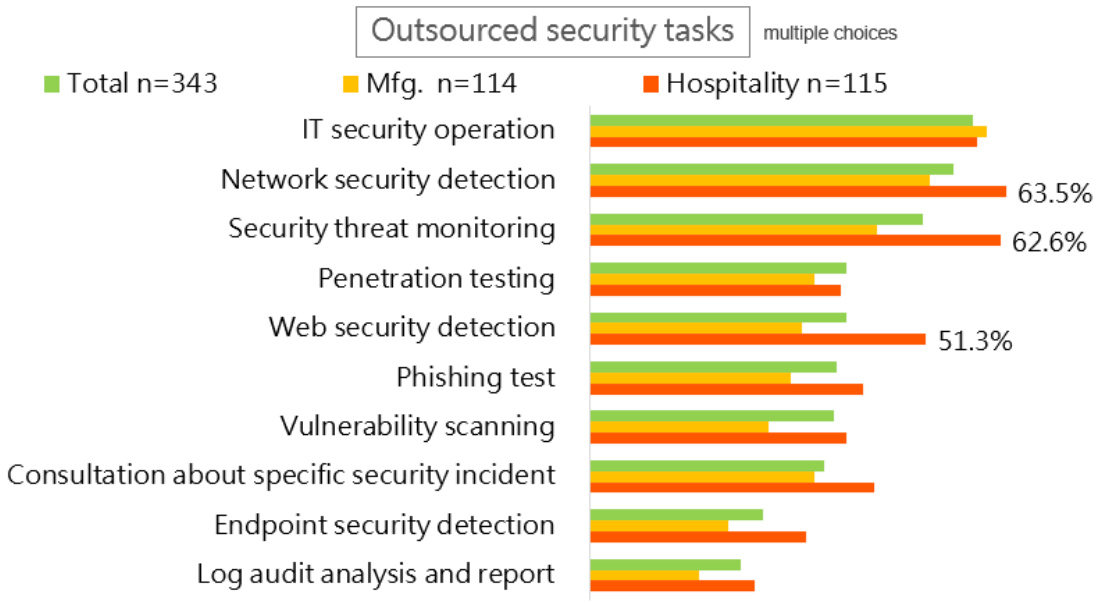
This tells us that companies rich in resources, such as large enterprises or IT departments with large staffing, have higher demand in outsourcing their IT system maintenance.



single choice
Source: This report (2020)

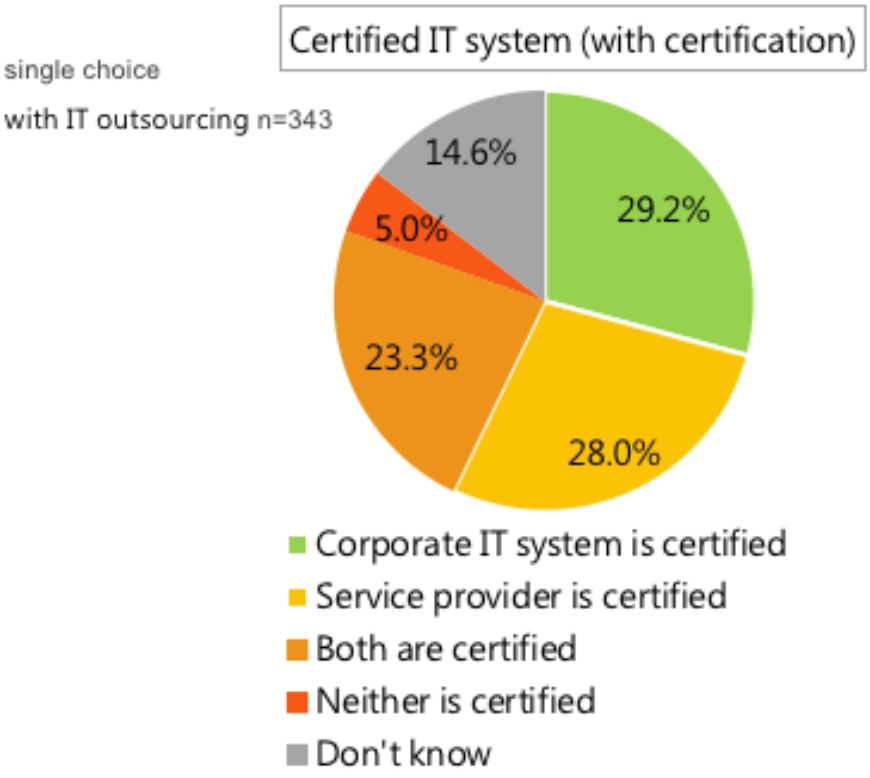
II Outsourced Security Tasks

When we asked companies about which services/maintenance tasks they have outsourced, 'IT security maintenance' tops the list (58.3%), followed by 'web security detection' (55.4%) and more than half are outsourcing their 'security threat monitoring' (50.7%) as well. To compare the results by industry, hospitality obviously has outsourced more tasks than manufacturing and others.

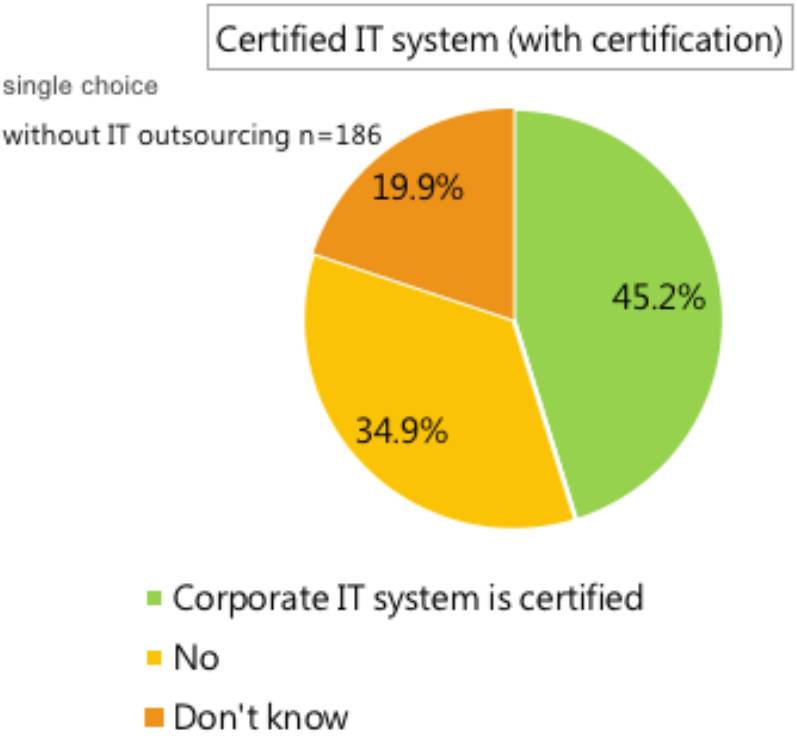


Source: This report (2020)

The result shows no apparent differences in the percentage between certified company systems and certified vendor solutions, the results are 40% and 50% respectively.



Source: This report (2020)



III Security Service Purchase/Rental/Subscription

In addition to outsourced IT maintenance, we also looked into the

products/services they have purchased or subscribed to understand security requirements. For purchased or subscribed services, 'firewall' comes first on the list, with the percentage as high as 80%+ , followed by 'antivirus' (77.5%). The third highest service, 'email filtering tool,' has more than 50%.

Businesses in manufacturing, with mostly B2B transactions, have lower demand in security comparing with hospitality service providers, which are more B2C in its nature. Manufacturers do not have as many assets/sensitive data that need protection. Hospitality, however, always accesses customers' personal information directly and it is the task of their entry-level staff or front-line service persons.

> *"We (the manufacturers) do not link to external network and we do B2B, not B2C. We have no customers on the front-line, but we serve our upstream buyers. Most of our clients also have their own way (of safeguarding system security.)"*

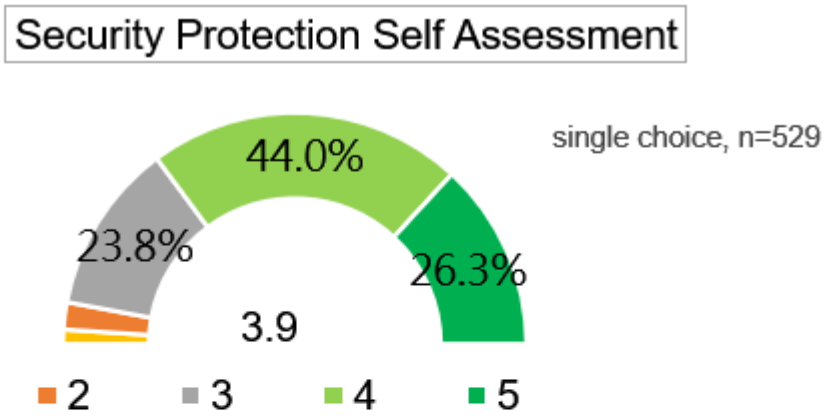
> *"In manufacturing, not many people need to get their hands on the core system. But for hotels, the very entry-level personnel will need to access the system. That's why personnel training is their priority."*

	Total n=343	Mfg. n=114	Hospitality n=115
Firewall	84.5%	85.4%	82.7%
Antivirus	77.5%	81.6%	72.7%
Email filtering tool	53.7%	56.8%	50.0%
Intrusion detection system/Intrusion Prevention System (IDS/IPS)	47.4%	41.6%	51.3%
Web application firewall (WAF)	41.0%	37.3%	50.0%
Data loss prevention tool (DLP)	32.1%	25.4%	42.7%
Security Operation Center (SOC)	30.8%	25.4%	28.7%
Database Activity Monitoring (DAM)	28.7%	25.4%	38.0%
Vulnerability Scanning	27.6%	20.5%	24.0%
Log Management	26.1%	21.6%	24.7%
Advanced Persistent Threat (APT) Protection	25.0%	20.5%	24.7%
Penetration Testing	22.3%	14.6%	22.7%
Security Health check	21.6%	17.3%	20.0%

Source: This report (2020)

IV Self-Assessment on Security Protection and Requirements Details

When asked to assess how well their security protection is, 44% opt for 4, and 26.3% rate it as 5. In summary, more than half give a score above 4, which shows they are well familiar and attentive to their IT system. Overall, the average score is 3.9.

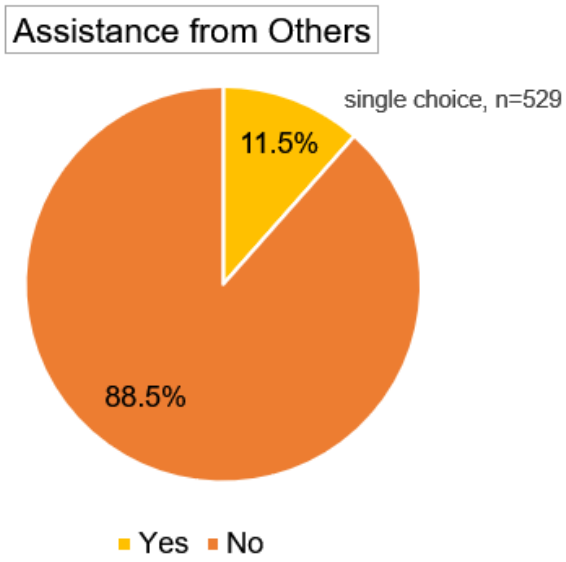


	Good security protection (4/5 points)	Average (points)
Overall n=529	70.3%	3.9
Mfg. n=185	58.9%	3.7
Hospitality n=150	78.7%	4.0

Source: This report (2020)

When asked about how security solution is implemented, only 10% seek assistance from external organizations like TWCERT/CC and a number of IT service providers such as Trend Micro, Athena Information Systems, DigiWin, Well Take Computer, IBM, and Microsoft.

Services they asked from vendors to provide include consultation, ERP implementation, implementation of mainframes or system solutions, cloud services, packet analysis, ransomware solution as well as outsourced system development.



Source: This report (2020)

V Security Requirement Details

In addition to how respondents assess their own security protection, the survey also looks into the level of demand on security services and finds that 'incident reporting and response' has the most demand (53.1%), followed by 'security consultation' (52.2%) and 'incident coordination and handling' (51.2%) All three security services demonstrate high level of demand with more than 50% of percentage. Hospitality has significantly higher demand than the other industries.

(Multiple choices)	Total	Industry Type			Business Size	
		Mfg.	Hospitality	Other	Large enterprises	SMEs
n=	529	185	150	194	282	247
Reporting and response	53.1%	48.1%	58.0%	54.1%	56.4%	49.4%
Security consultation	52.2%	52.4%	60.7%	45.4%	52.8%	51.4%
Incident coordination and handling	51.2%	45.9%	56.7%	52.1%	54.6%	47.4%
Information consolidation	47.4%	42.7%	44.7%	54.1%	51.4%	42.9%
Information sharing	37.6%	35.7%	38.0%	39.2%	43.3%	31.2%
Seminar	33.5%	32.4%	37.3%	31.4%	37.6%	28.7%

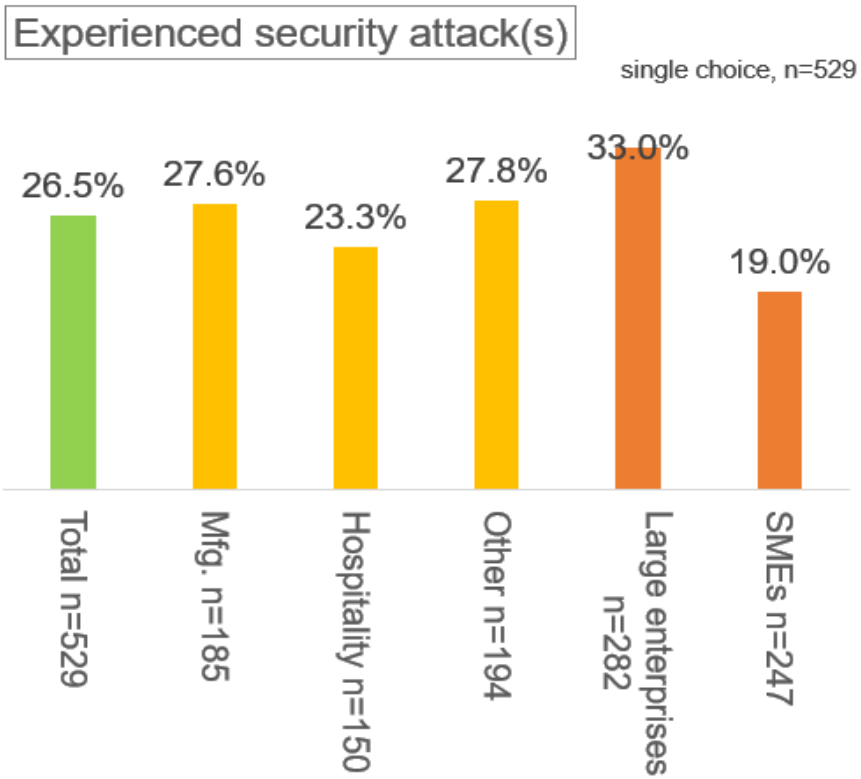
Source: This report (2020)

Chapter IV. Security Incidents and Awareness Planning

Chapter IV. Security Incidents and Awareness Planning

I Cyber Attacks and Damages

The result shows 26.5% of the enterprises suffered 'security attacks' in the past. More than 30% of the large companies whose IT department is staffed 11+ have encountered this problem. This means the larger the business size, the easier it becomes the target.



Source: This report (2020)

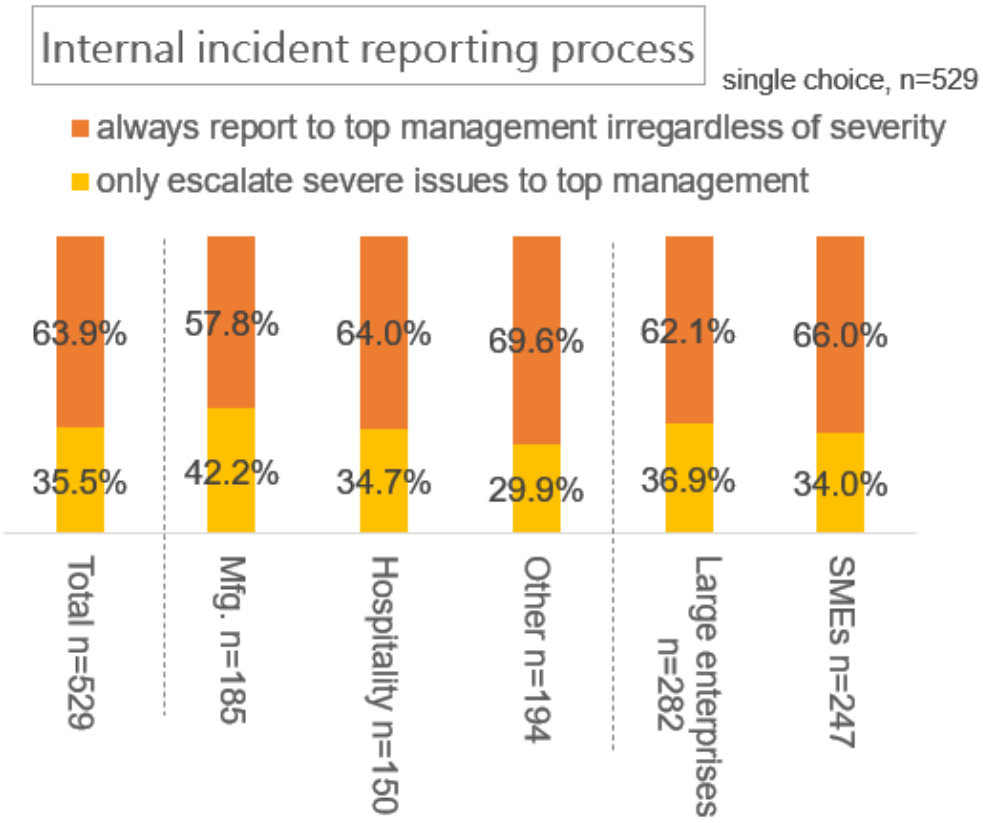
45.7% say the biggest impact is 'interrupted business or services,' found particularly in hospitality. The next in the row is 'increased implementation cost' with 33.6%, especially for manufacturers. As for attacks with more severe impact, revenue loss is common.

Damages caused by incidents (multiple choice)	n=140
Interrupted business or services	45.7%
Increased cost for security implementation	33.6%
Lost or stolen corporate data	20.7%
Lowered employee productivity	17.9%
Damage to corporate image	17.1%
Loss of revenue and business opportunities	13.6%
Delayed shipping	11.4%
Monetary loss	8.6%
Legal problems	8.6%

Source: This report (2020)

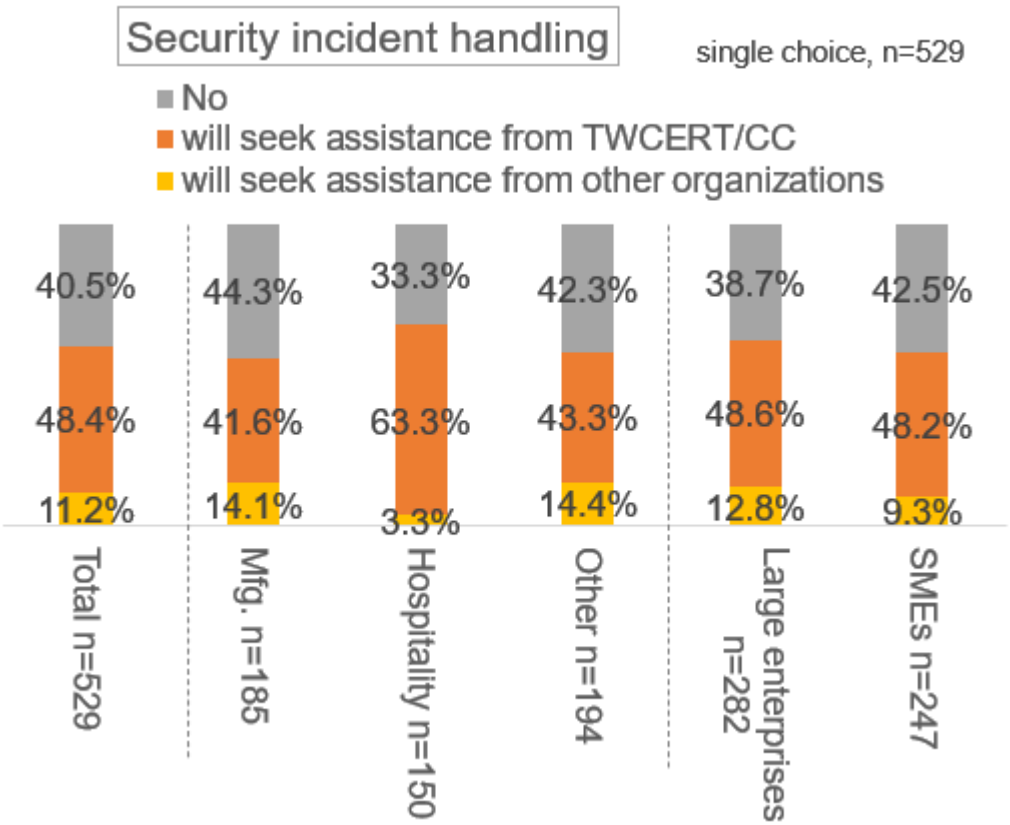
II Security Incident Reporting and Solution Assistance

Regarding the internal process for reporting incidents/attacks, 63.9% say they always escalate the issue to business owners irregardless of severity. This shows the majority of companies report incidents to their highest level of management in the incident handling mechanism.



Source: This report (2020)

In the event of security incidents, half of the enterprises will ask TWCERT/CC for help, especially businesses in hospitality. The percentage does not differ by size of business. In contrast, 40.5% of the companies do not seek help from external organizations, mainly businesses in manufacturing and SMEs.



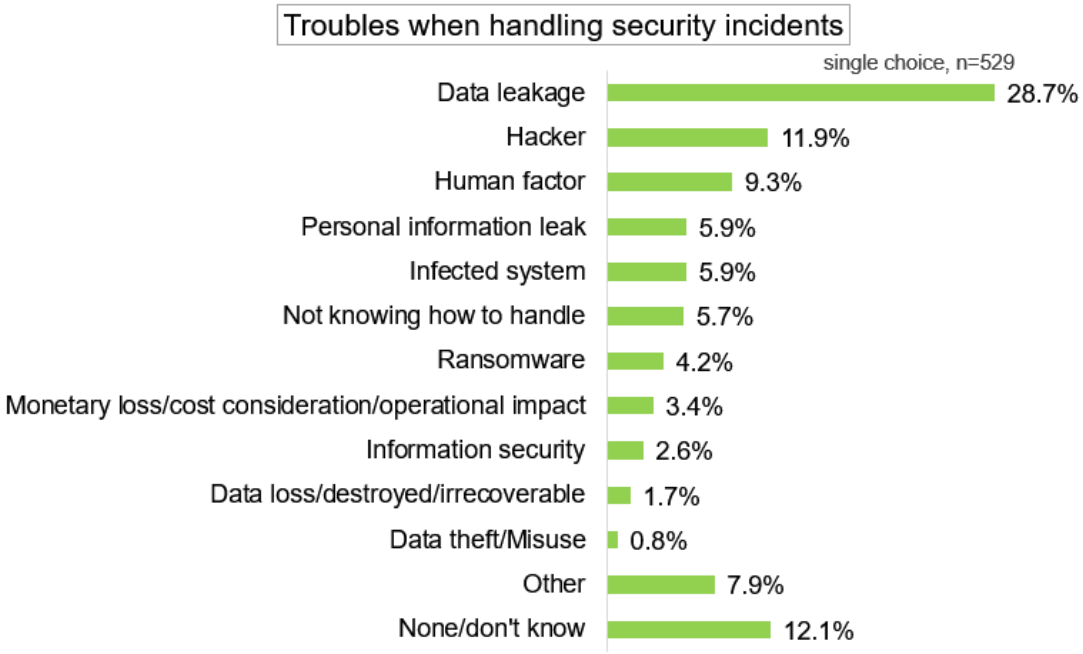
Source: This report (2020)

III Security Concerns

Whether the respondents have encountered security attacks previously, their biggest concern is unanimously the 'data loss' (30%) ─ the exposure of confidential data or customer/operation data leakage could subsequently impact daily operation/production.

Another 10% are concerned about 'cyber attacks,' including being hacked, system intrusion or DDoS.

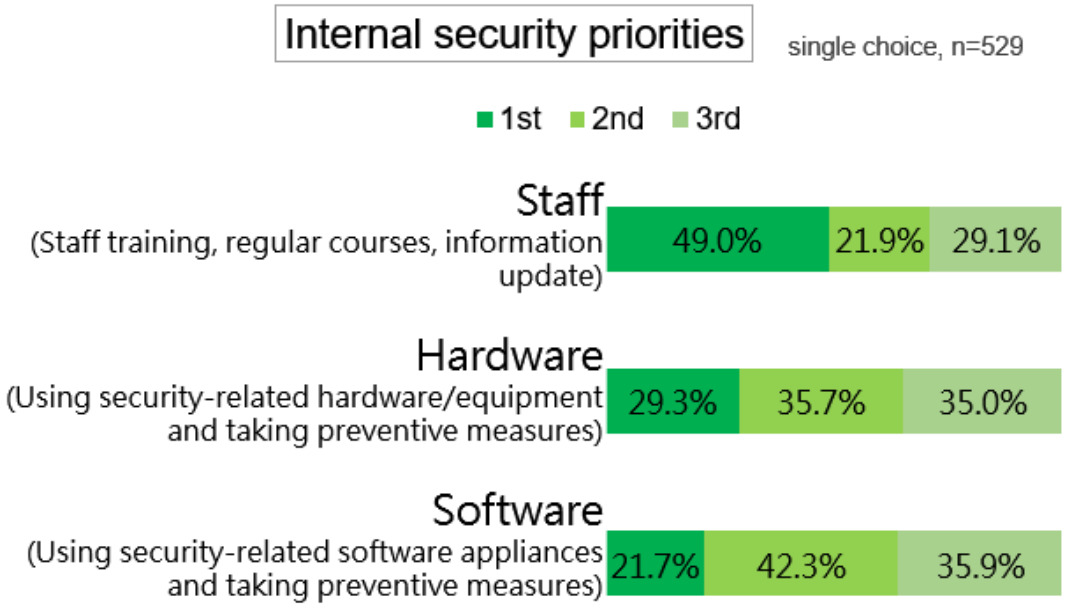
Nearly 10% are also worried about 'human factor,' meaning staff who lack of awareness or conceal the cyber attack without reporting.



Source: This report (2020)

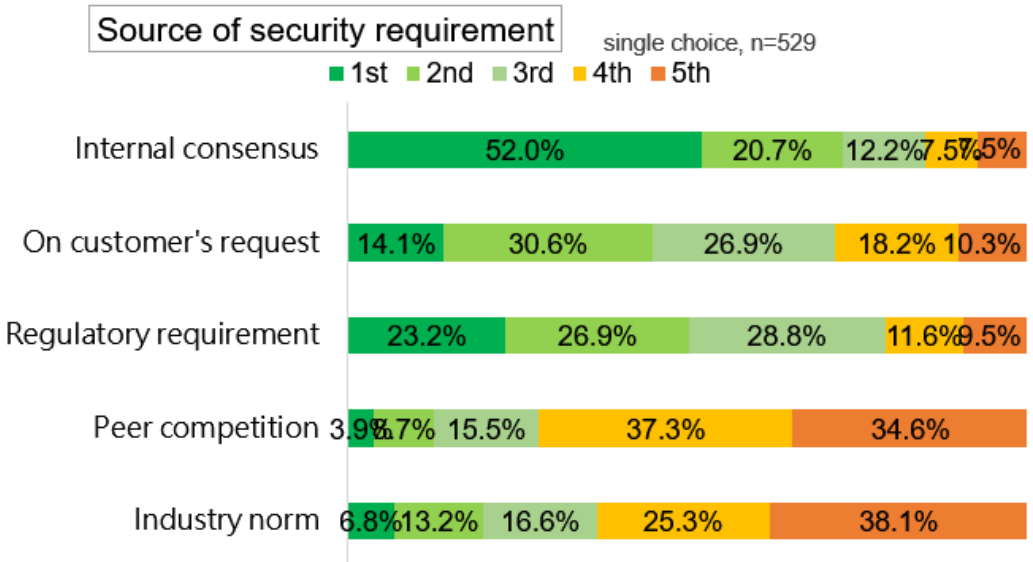
IV Enterprise Security Planning

Items to be selected/prioritized in internal security plans include 'staff', 'hardware' and 'software.' 'Staff' has the highest percentage, meaning corporations value employees' security literacy the most. Those who work in other industries and IT department staffed with 11+ show higher percentage than others.



Source: This report (2020)

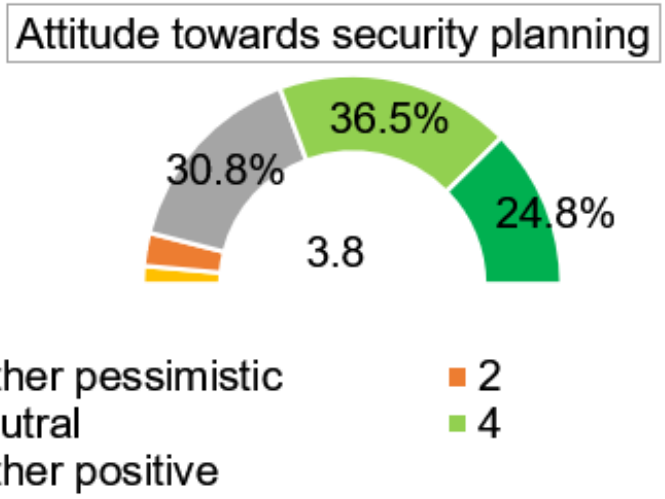
As to where corporate security requirements are from, 'internal consensus' tops the list because more than half of the respondents mark this as the first, followed by 'regulatory requirement.' In comparison, 'competition within the industry' and 'industry norm' are two weaker motives.



Source: This report (2020)

V Attitude towards Security Planning

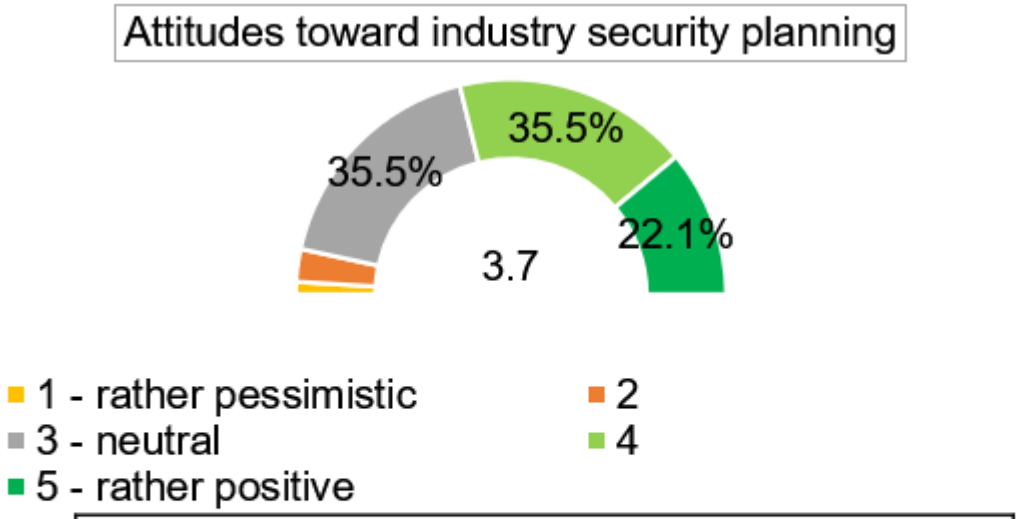
Concerning industry security awareness, a scale of 1 to 5 is used to evaluate the pro-activeness in security planning of the company's decision makers, the attitudes of industry peers and upstream/downstream business partners. For pro-activeness within one's own organization, the majority of respondents rate it as 4 (36.5%) or 5 points (24.8%) and the average score is 3.8



	Positive (4/5 points)	Average
Overall n=529	61.2%	3.8
Mfg. n=185	51.9%	3.6
Hospitality n=150	66.0%	3.8

Source: This report (2020)

As to industry-wise attitude, the majority also gives 4 (35.5%) or 5 (22.1%). The average score is 3.7. We can conclude that the attitude towards security planning does not differ much, whether within one's own organization or industry-wise because they all appear to be positive.



	Positive (4/5 points)	Average
Overall n=529	57.7%	3.7
Mfg. n=185	47.0%	3.6
Hospitality n=150	63.3%	3.8

Source: This report (2020)

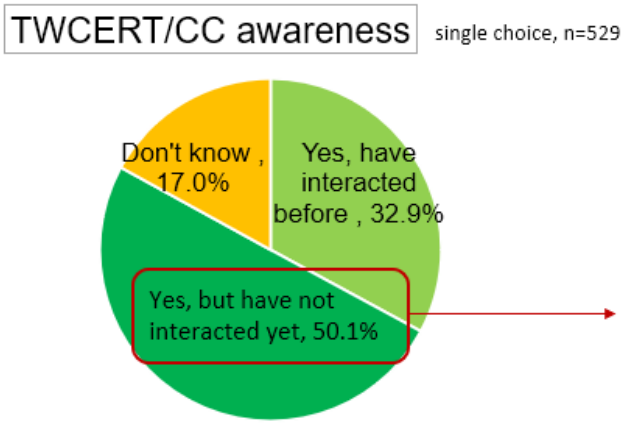
Chapter V . TWCERT/CC Recognition and Interaction

Chapter V. TWCERT/CC Recognition and Interaction

I Awareness and Interaction

Among the authorized staff in charge of maintenance/management/IT system decisions and working in companies with Internet-connected systems, 83.0% know about TTWCERT/CC. 30% have interacted with TWCERT/CC before and they are mainly businesses in hospitality, large businesses, or IT department with 11+ staff.

50% are aware of the organization but have never contacted them before. 17.0% have not heard of TWCERT/CC and they are mostly manufacturers or IT departments with less than 5people.



Reason for no interaction	n=265
No such demand yet	52.1%
Do not know how to contact TWCERT/CC	35.1%
Not familiar with TWCERT/CC services	31.7%
Have no intention to	9.4%
Other	1.5%

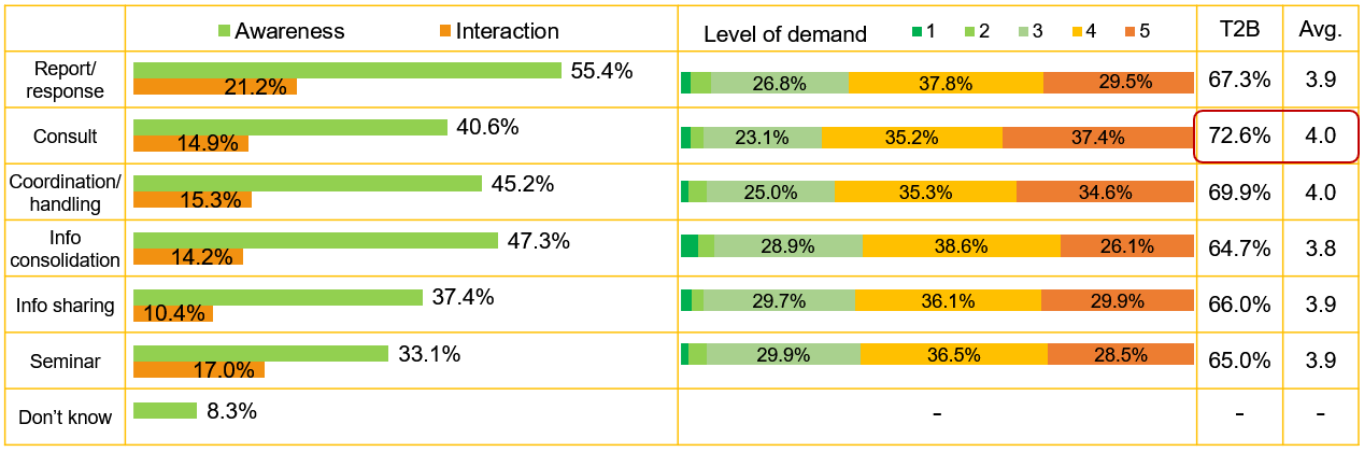
Source: This report (2020)

II Awareness/Interaction/Security Demand

'Incident reporting and response' is the most recognized TWCERT/CC service, with 55.4% of the respondents aware of it, particularly large enterprises or IT department staffed with 6-10 people. The second well-known service is 'information consolidation' with 47.3% of recognition. For this service, TWCERT/CC consolidates domestic and overseas

security information and has it published for enterprise users and the general public.

Despite its highest demand, 'security consultation' only has 15% of interaction. But 'information sharing' is the service with the lowest interaction rate.

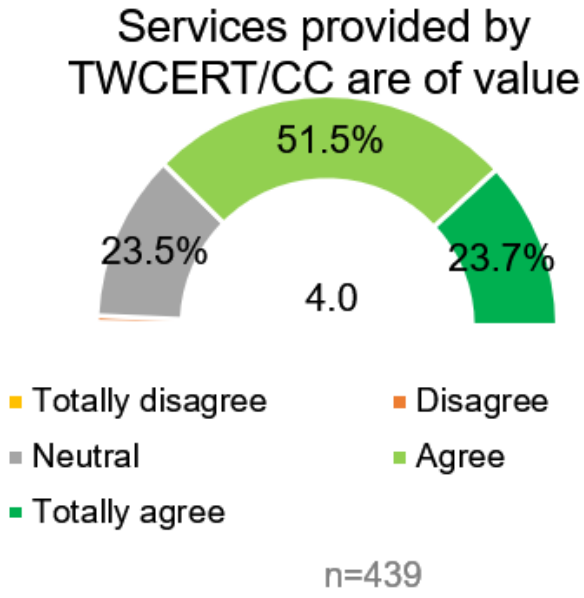


n=529

Source: This report (2020)

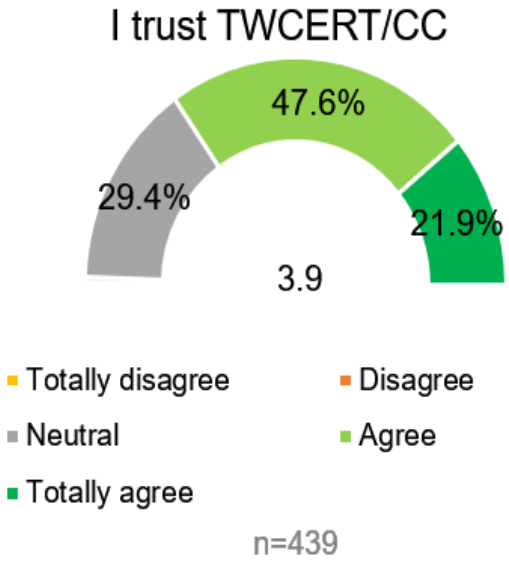
III Overall Satisfaction/Sentiment towards Service Value

For respondents aware of TWCERT/CC, 75% recognize TWCERT/CC's work and find their services of value. Hospitality, large businesses, IT department staffed with 5 ↓ or 11+ give ratings higher than average.



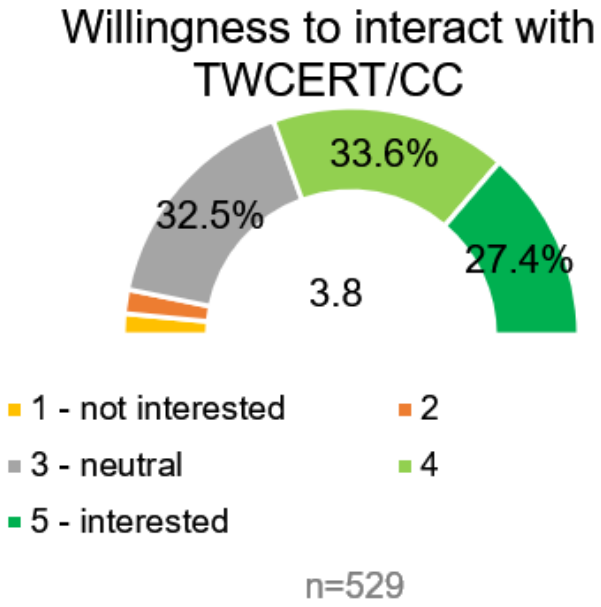
Source: This report (2020)

70% trust TWCERT/CC. Large enterprises and IT department staffed with 11+ give higher reviews than others.



Source: This report (2020)

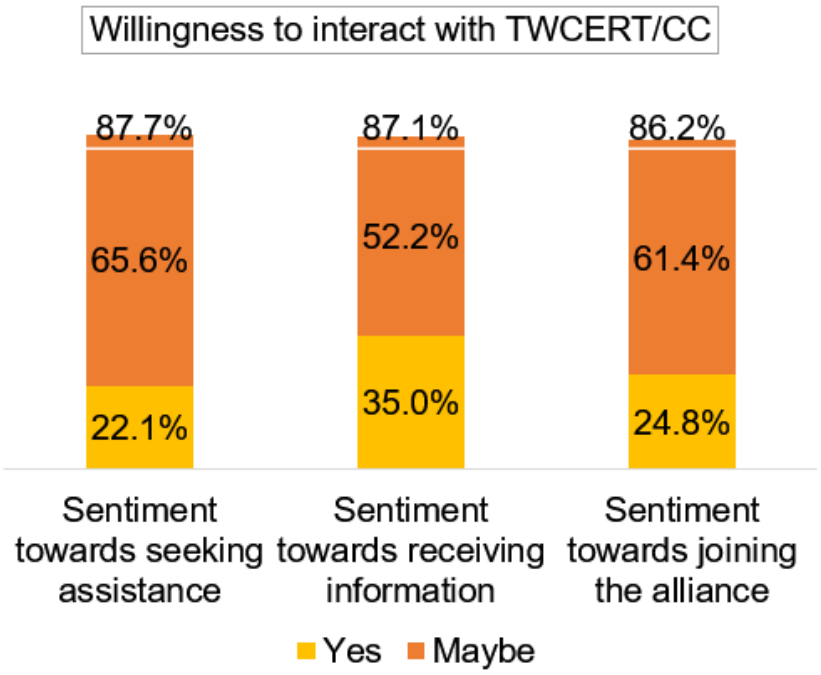
Overall, 61.1% demonstrate willingness to have more interaction with TWCERT/CC in the future. Hospitality, large businesses, IT department staffed with 6+ give ratings higher than average.



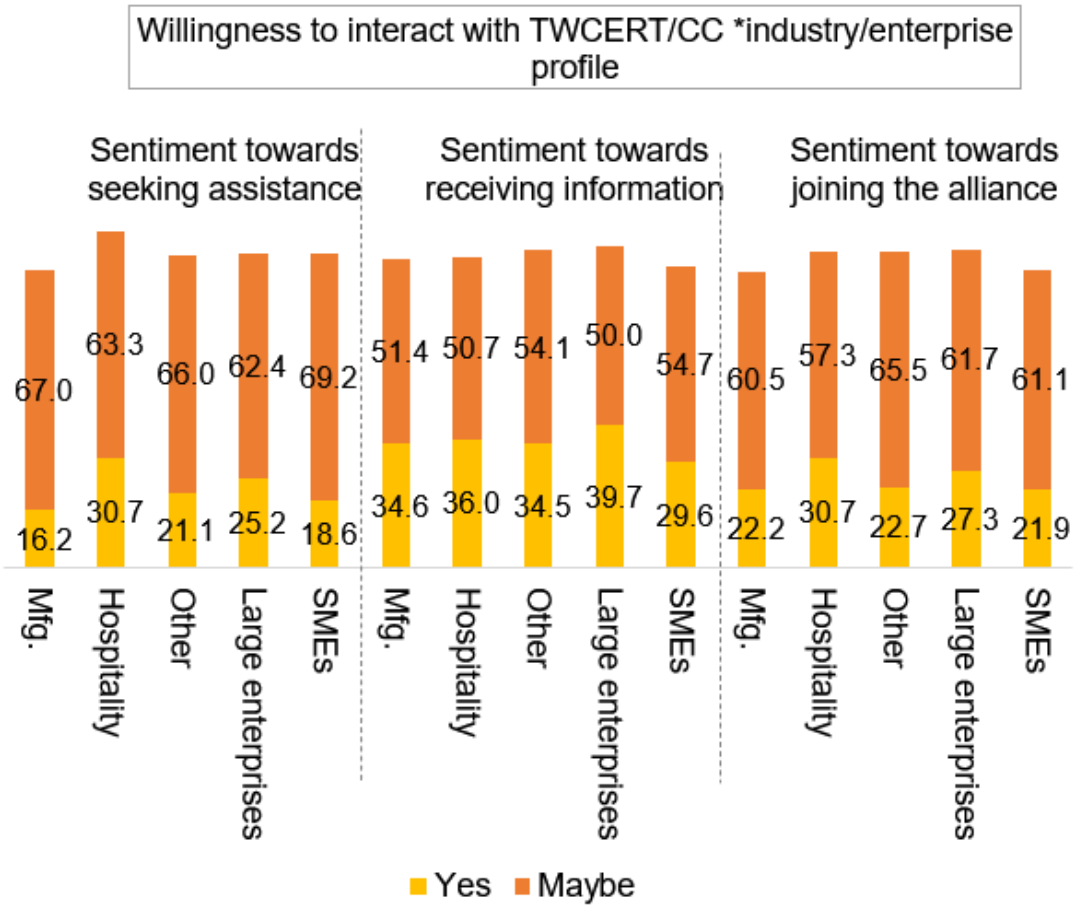
Source: This report (2020)

IV Building Reciprocal Relationships and Future Development of Security Reporting

With respect to willingness to interact, 'seeking assistance' (87.7%) has the highest percentage, followed by 'receiving security information about his/her company's products from TWCERT/CC (87.1%).



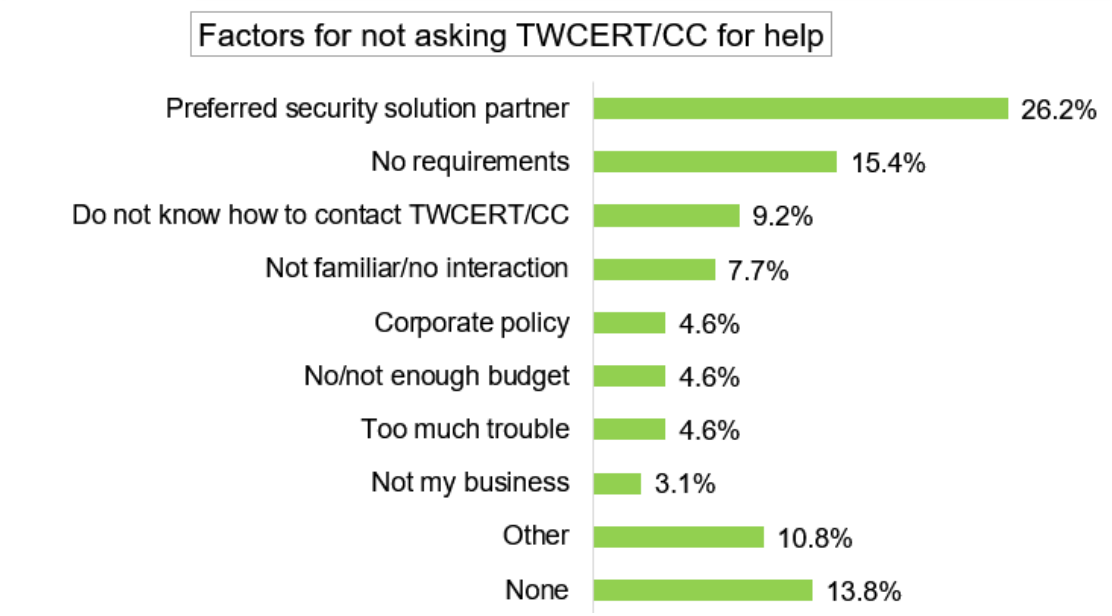
Source: This report (2020)



Source: This report (2020)

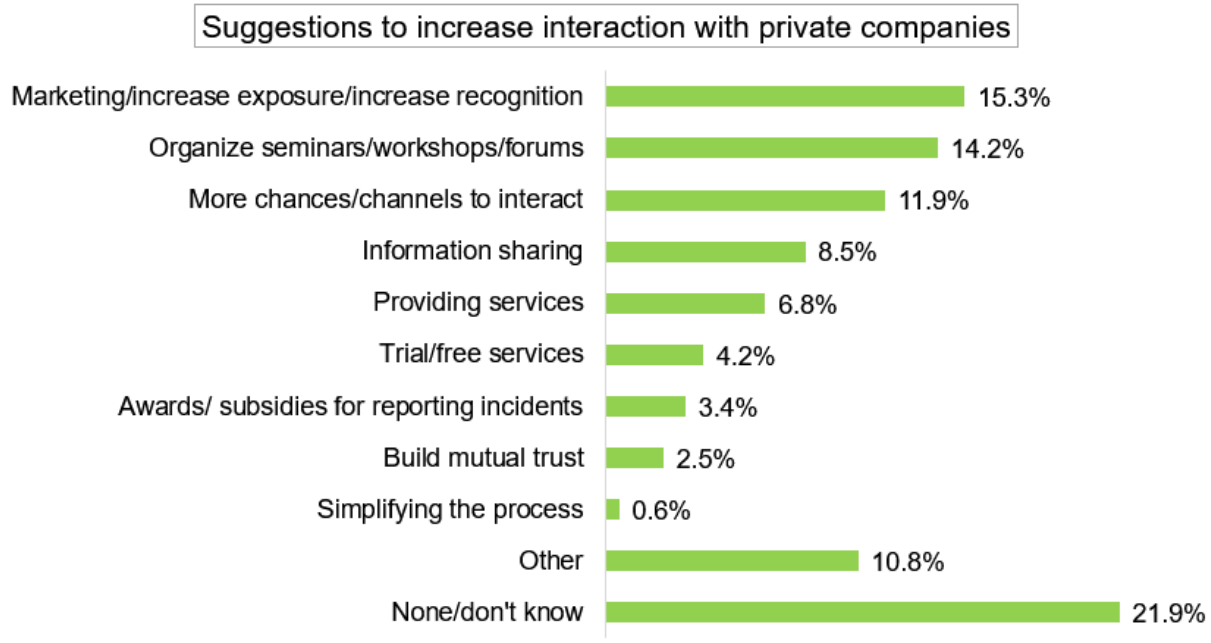
V Future Directions of Interaction

We asked a follow-up question for those without intention to seek assistance from TWCERT/CC about the reason. 26.2% say they already 'have a preferred security solution partner.' For example, they would ask their superior organizational unit for help, they have a designated department in charge of security, or they have already got a security solution vendor. Another 15% say they don't have any security incidents now, so no assistance is required.



Source: This report (2020)

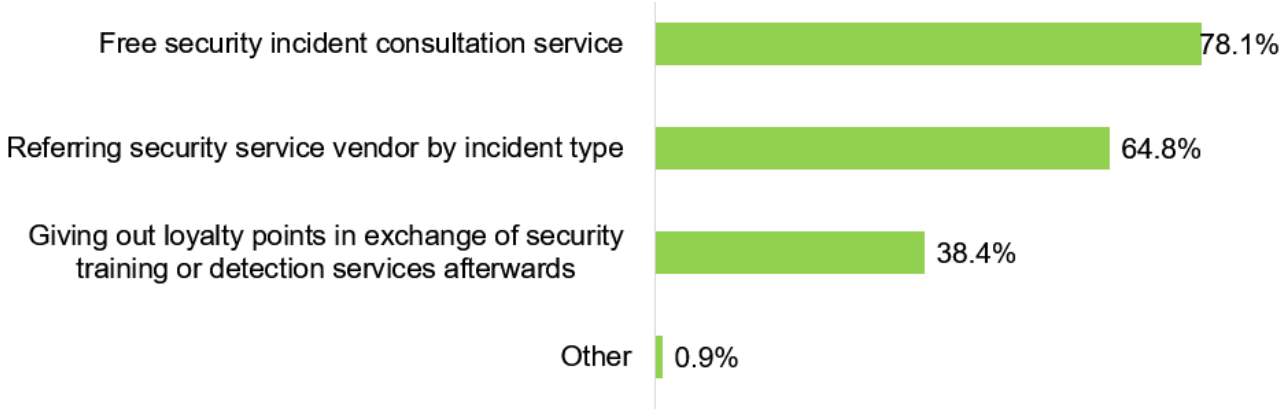
When asked about how TWCERT/CC can increase interaction with the private sector and make them willing to report incidents, 15% suggest TWCERT/CC to work on 'marketing/increase exposure/increase recognition.' For example, TWCERT/CC should make themselves known to the public, introduce themselves to the enterprises about what their services can do and what kind of assistance they can offer after incidents are reported and even work with governmental agencies to promote security literacy. In addition, 14.2% suggest TWCERT/CC to organize seminars, workshops and forums, so they can have more interaction with security personnel from different companies.



Source: This report (2020)

VI Incentives to Seek Assistance

To our respondents, 'free security incident consultation service' is the most attractive incentive for them to approach TWCERT/CC in the event of incidents. The percentage is as high as 78.1% and this is found particularly in companies whose IT department has less than 5 staff.



Source: This report (2020)

Build relationship in an orderly manner

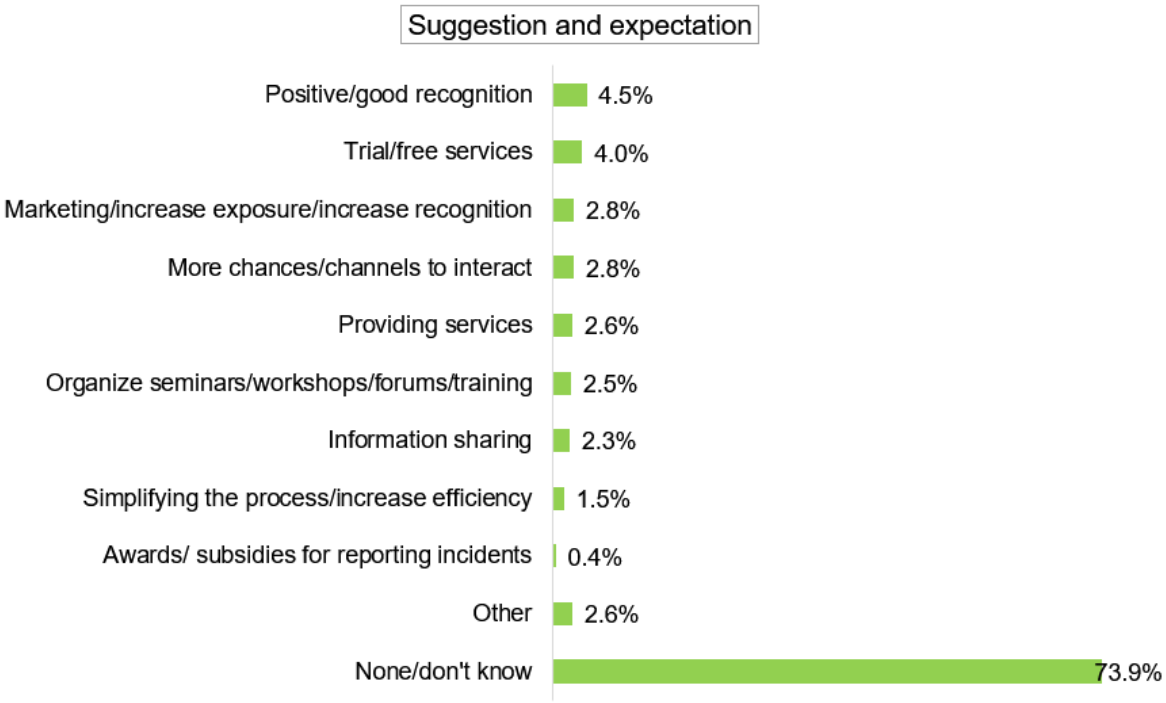
> *"For the initial stage, there should be online or physical ads to attract SMEs. You can start with services like vulnerability scanning to win their trust first. Once trust is built, people will think of or go to TWCERT/CC when they are in need. I am talking about SMEs. They are the ones that need more governmental support."*

VII Suggestion and Expectation

When asked about suggestions and expectation for TWNIC or TWCERT/CC, quite many give positive reviews and encourage TWNIC and TWCERT/CC to become excellent security leader outperforming competitors with its expertise.

Secondly, respondents also hope TWNIC and TWCERT/CC to provide 'free trial/ free services' ─ annual security check/consultation services around Taiwan, free consultation and assistance, free subscription of reporting information etc.

Some respondents have mentioned TWCERT/CC should work on 'marketing/increase exposure/increase recognition.' For example, TWCERT/CC should make themselves known to the public by making YouTube videos to promote the importance of security. Once people are aware there's an organization called TWNIC, they will approach TWNIC when they need the services/when they are interested.

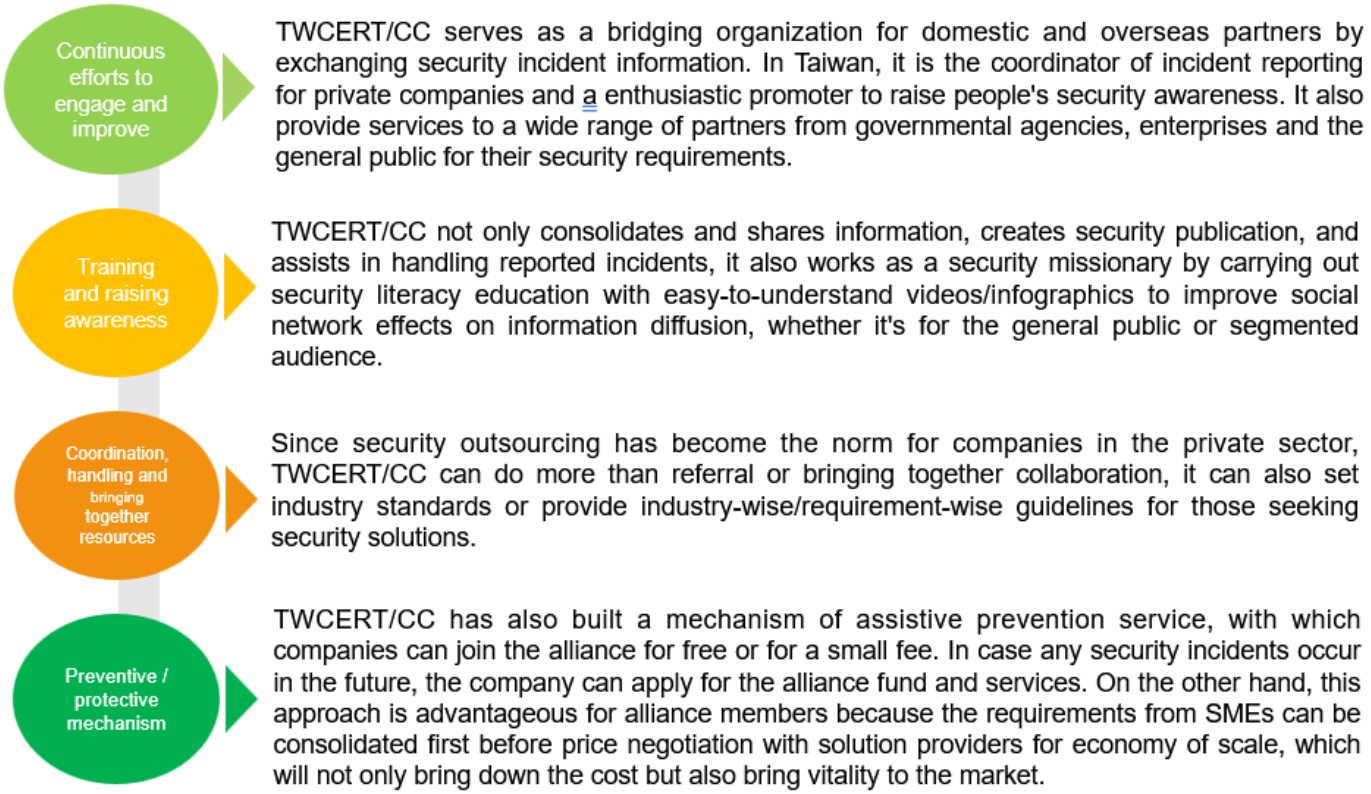


Source: This report (2020)

Chapter VI. Recommendations

Chapter VI. Recommendations

Goal: short-term: Promoting Incident Coordination and Handling
Long-term: Establishing Preventive and Protective Mechanism



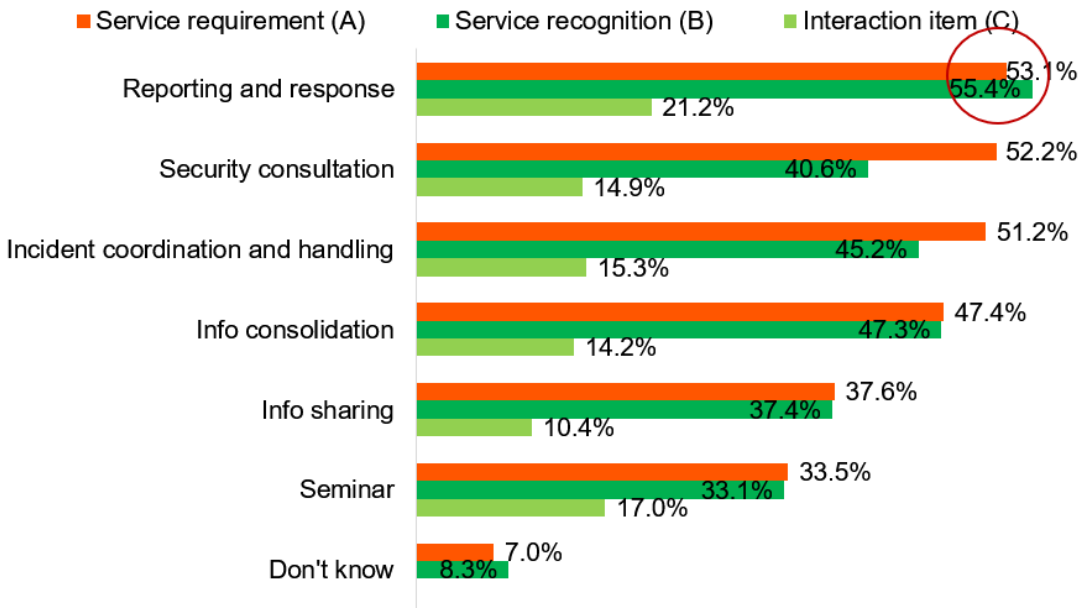
I To Continue Providing Security Consultation Services/Sharing Info/Identify Service Req. from the Surface Downward

83.0% are aware of the existence of TWCERT/CC. 32.9% have had interaction with it, whereas 50.1% are only aware of the organization but never have any interaction before. Reasons for not having any interaction include having no such demand, not knowing the contact info and not familiar with TWCERT/CC services.

‘Report and response’ not only has the highest service demand rate, but also has the highest service recognition rate and the most interaction.

The high interaction rate shows TWCERT/CC's incident report and response service strikes to the core and fulfills the actual enterprise need.

From the interviews, we found respondents might have heard about the name of TWCERT/CC, but not necessarily familiar with what it actually does. When they do interact with TWCERT/CC, they do not always contact the person in charge of incident report and response. Instead, more than half of the respondents contact TWCERT/CC for 'security consultation', but the actual interaction rate is as low as 15%. Despite nearly 40% of demand and awareness, 'information sharing' only has 10% of interaction rate.



Source: This report (2020)

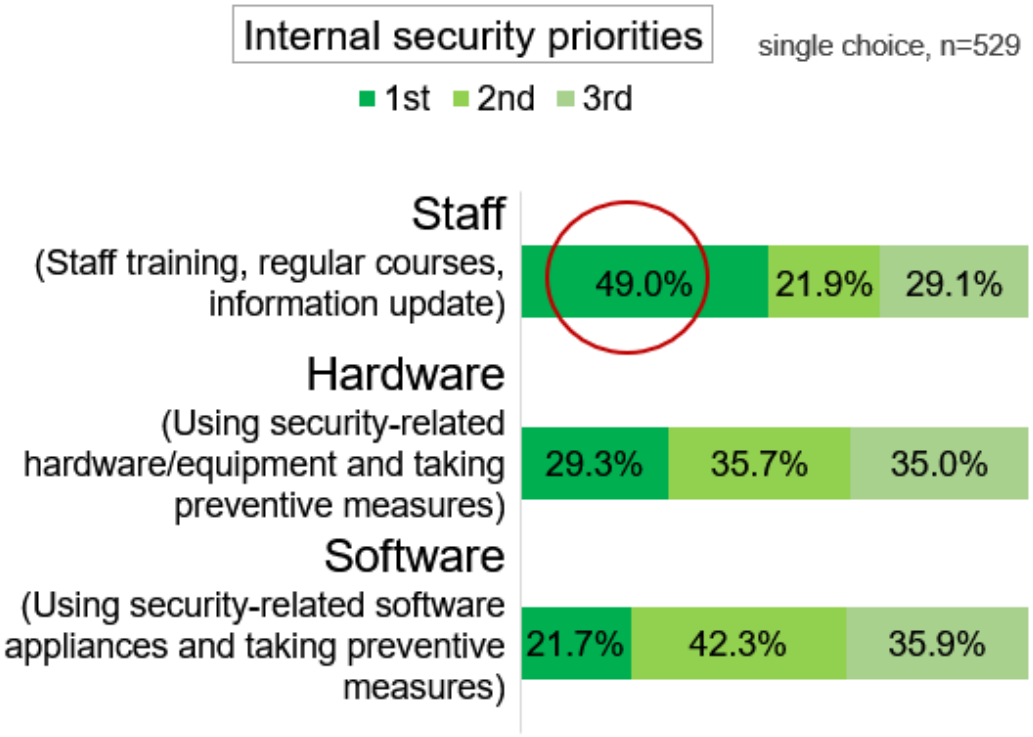
	Req. fulfillment rate[3] (C/A)	Interaction conversion rate[4] (C/B)
Reporting and response	39.9%	38.2%
Security consultation	28.6%	36.7%
Incident coordination and handling	29.9%	33.9%
Info consolidation	29.9%	30.0%
Info sharing	27.6%	27.8%
Seminar	50.8%	51.4%

Source: This report (2020)

II To Provide Diverse Education/Training from Security Literacy for Employees to Nationwide Security Education

When it comes to the company's attitude towards security planning, 'staff training', 'regular courses', and 'information update' are the top priorities. This coincides with the point given by one respondent from the convergence analysis ─ 'Cyber-security has become common sense. In the past, security topic might be some sort of knowledge or expertise that is nice to acquire. However, as the network technology is advancing at incredible speeds, now security literacy is equal to the common sense that everybody should have.

[3] Requirement fulfillment rate is the level of interaction between people who need the services and TWCERT/CC.The higher the percentage is, the more the requirement is fulfilled.
[4] Interaction conversion rate is the the level of interaction between people who are aware of the services and TWCERT/CC.The higher the rate is, the more people who know about the services also use them.



Source: This report (2020)

A. Enterprises to proactively enhance the employees' security literacy

In addition to regular training courses and seminars, some companies send phishing emails to their employees to check if they stay alert with potential security threats and include security awareness as part of performance review.

> *"Security training, no matter how many hours are required in a year, is made compulsory for users. Despite taking all the mandatory courses, some of them still get fooled by the phishing email we sent. When an employee takes the bait, there will be punishment - more security training and a demerit in performance review, which might affect their bonus amount."*

B. Offer diverse training courses based on the requirements

For hospitality businesses, their entry-level staff or front-line service persons will have direct access to customer personal information. Therefore, they put strong emphasis on entry-level staff's training. Besides giving in-person lectures for training, developing training materials in a user-friendly, easy-to-share way also fosters the enhancement of employee security literacy.

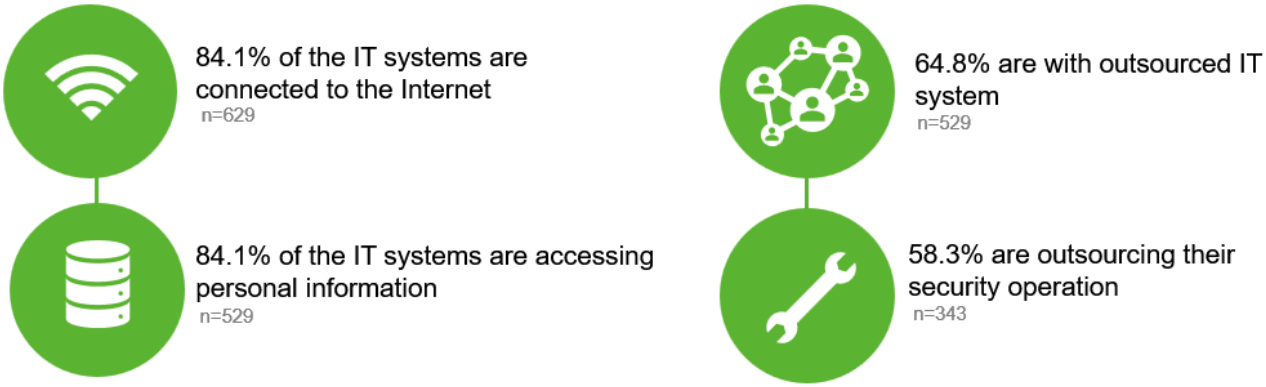
> *"IT personnel could be the cause of security issue because IT staff has the highest level of authority to the system. If this person lacks proper security literacy, he/she is the system vulnerability himself/herself. If IT staff is well equipped with security awareness, they can also give lectures and help colleagues from other departments. If you ask a manager to attend the training, he/she will not pass on the information to others."*

> *"Take incident reporting for example, people with no knowledge about this topic won't even bother to check what it is. Since this is the service we are offering, we could come up with a more effective way in delivering the information, could be push notification, or send (animated) videos to people's mailbox instead of an article. People don't have much patience reading through articles."*

C. Getting certified means the company attaches significance to security protocols

Whether the company outsources security services, more than 40% have been certified. This means even though some companies have already outsourced their IT system to spread the management risk, in general, they still value the importance of the standard protocol of security management.

III With Half of the Enterprises at Risks, it is Imperative to Understand the Req. and Create Industry Guidelines



Source: This report (2020)

A. All industries are facing security risks0

57% of the enterprises have IT system and their Internet connection rate/personal information access rate are more than 80%

Among all, more than 70% of the businesses have IT systems in the following four industries - finance and insurance, information and communication, electricity and gas supply and manufacturing. Unlike companies in the first three business types, who already have IT security audits conducted by their respective competent authorities, businesses in manufacturing are of the highest security risk. Besides, risks facing hospitality businesses are also higher than average.

B. IT outsourcing is common and requirements iffer greatly. However, there are no industry uidelines to follow or to be used as reference.

With sufficient technical manpower and rich resources, large enterprises are more capable of selecting appropriate vendors because they constantly face high level of risks. To release the burden of manpower

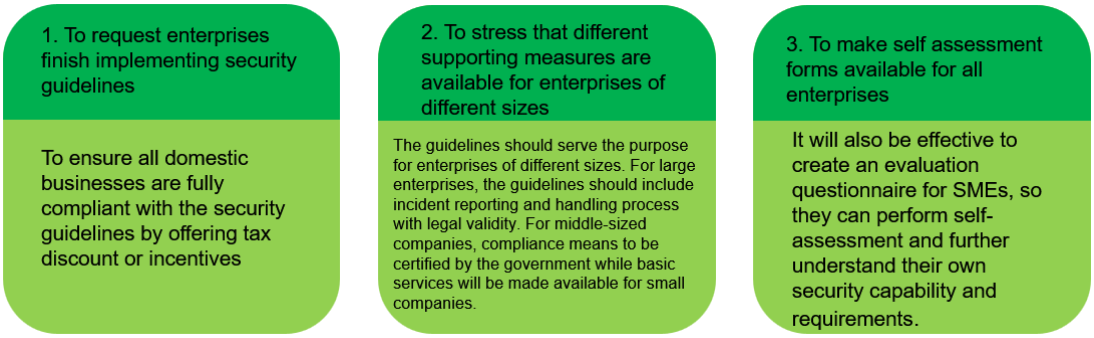
and spread the risk, purchasing or subscribing professional security software turn out to be a better solution for them.

SMEs, in contrast, do not have as many resources and have no guidelines to follow. They might have a hard time choosing the right vendor because they have concerns about being overcharged or not able to afford the software or having no funds to handle security breach.

C. Pushing Forward Industry Guidelines

The guidelines should define straightforward system security specifications compliant with global standards. Besides, they should be simpler than ISO 27001 standards, so it's easier for SMEs to be certified. The guidelines should also be the Taiwanese equivalent to EU/USA security standards, so as to increase Taiwanese companies' competitiveness when they promote businesses in the global market with recognized Taiwanese security capabilities.

Application process will include:



IV Legal Awareness in Security Training and Specific Assistive Prevention Service Plans

While security-related laws and regulations continue to evolve, enterprises should also keep up and stay up to date with the latest legal developments more quickly by continuously improving their own security capabilities and striving for healthy and sound social function on the Internet. Therefore, security-related laws will also be a part of

security literacy.

On one hand, TWCERT/CC can help enterprises fully understand the legal framework so they can urge internal security response. On the other hand, TWCERT/CC can report current business practices and scenarios to the legislative organization for them to identify the catalyst/friction for business development to further foster win-win cooperative relations.

To accommodate private companies' outsourcing requirements, TWCERT/CC can do more than security service vendor referral and recommendation. It can address the needs by building a mechanism of assistive prevention service, in which companies can join the preventive mechanism for free or for a small fee. In case any security incidents occur afterwards, the company can access the fund and services provided by assistive prevention first. On the other hand, TWCERT/CC can take the opportunity to offer more comprehensive services, understand company-specific requirements and help companies develop the habits of proactive incident reporting for better interaction.