
hkirc
香港互聯網註冊管理有限公司

Cybersecurity Awareness about Emerging Risks 2022

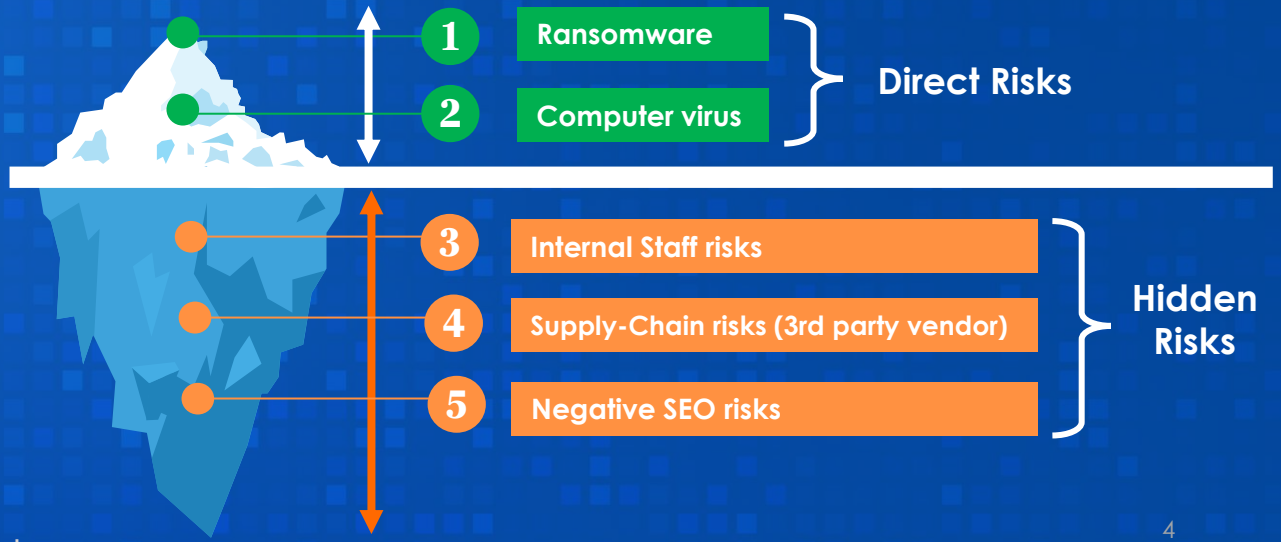
Market research result
2022

Research Objective

Cybersecurity covers a wide range of topics, including direct cyberattack (e.g. virus/ ransomware) but also some **hidden** emerging risks, including the three topics chosen in this study.

This study aims to understand the current situation of Hong Kong companies towards the **three emerging risks**.

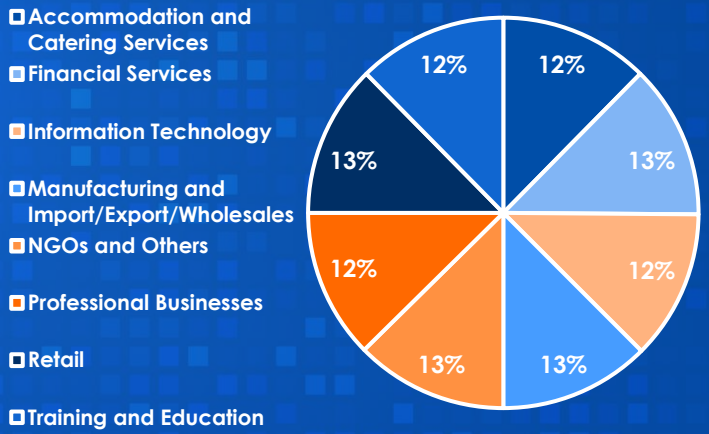
1. **Awareness Level**
2. **Risk Level**
3. **Protection Measures**



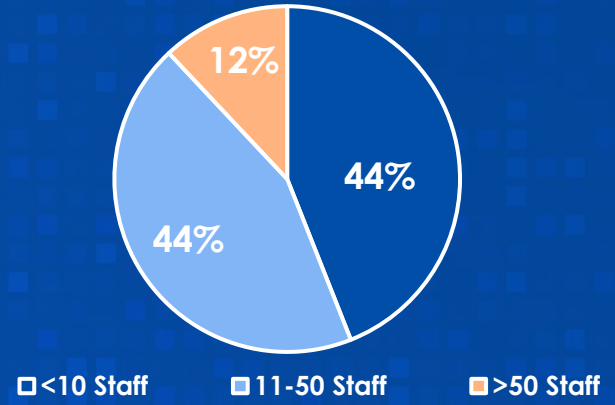
Research Background

- **Target:** Decision Makers/ IT Managers
- **Total Respondents:** 824 Responses
  (Data collection via telephone interview in July 2022)

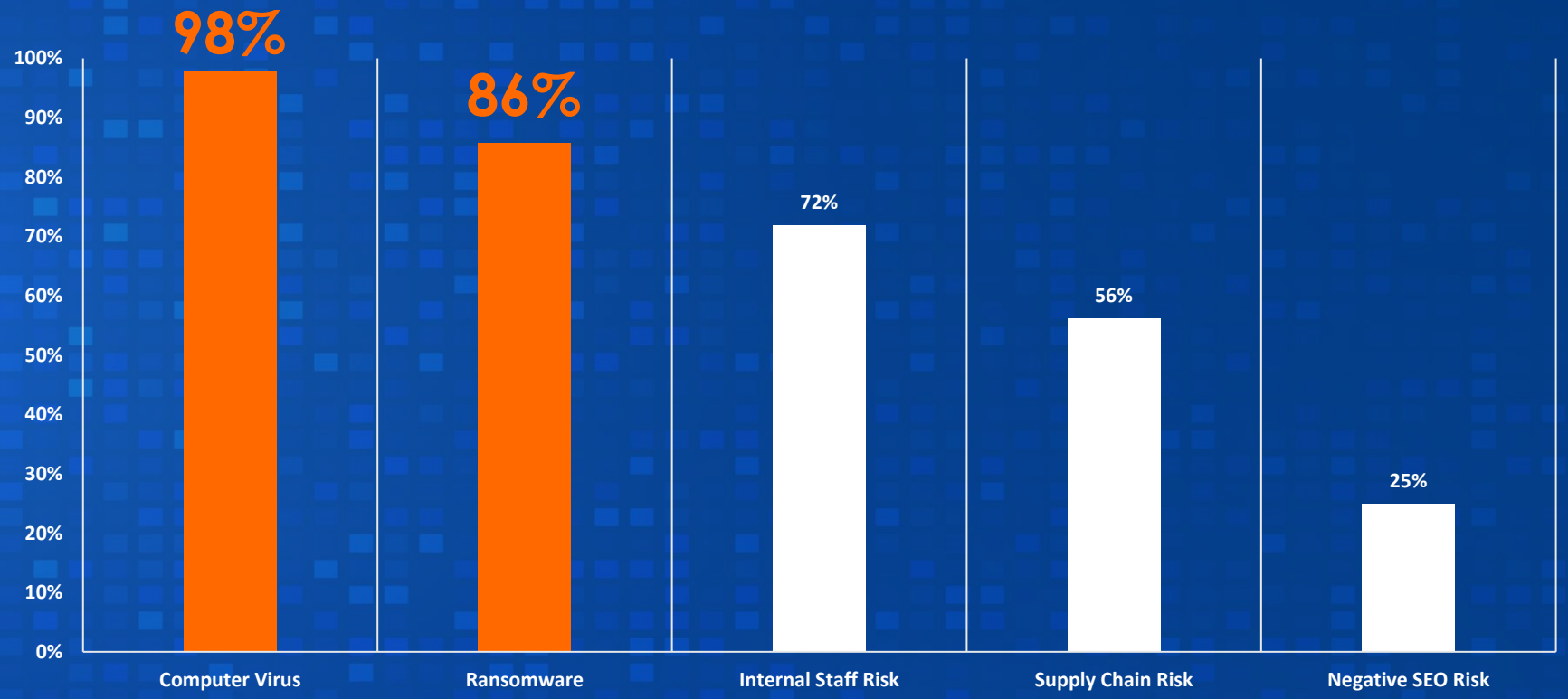
By Business Sector



By Size of Company

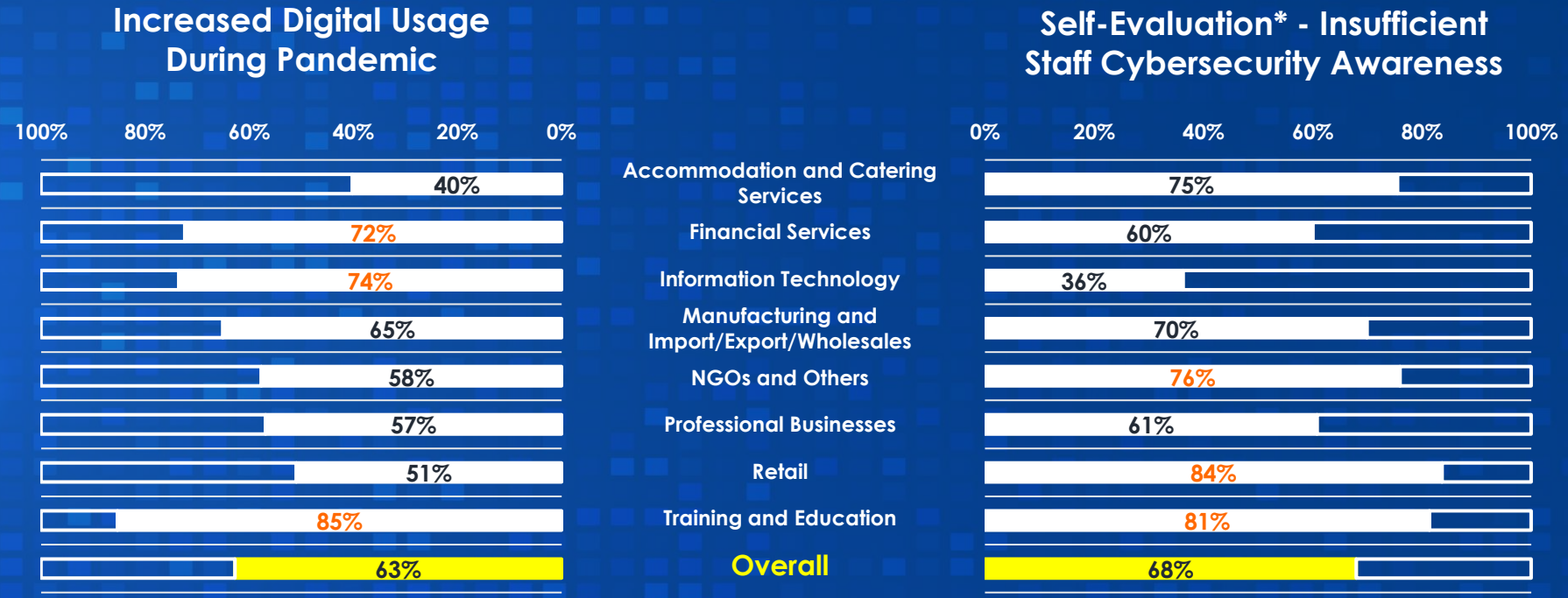


Awareness Level of Emerging Risks



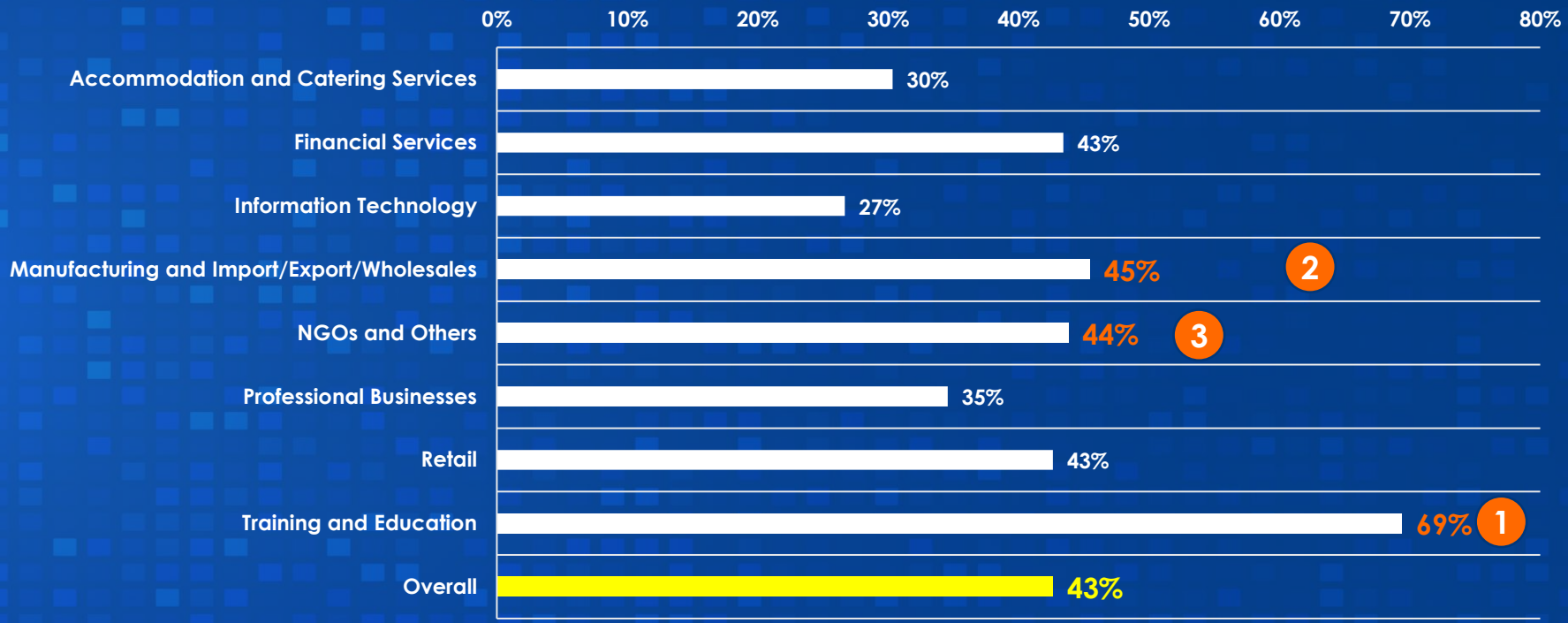
Internal Staff Risk

Internal Staff Risk Level



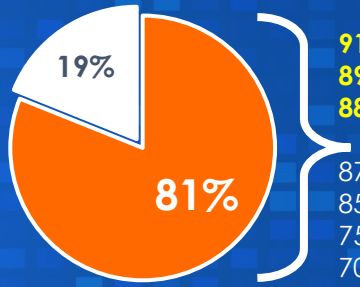
* Note: Assessment based on past experience (carefulness of staff/ any incidents happened/ current practice/ etc)

Internal Staff Risk Level



Internal Staff - Protection

Did Not Provide Regular Cybersecurity Training

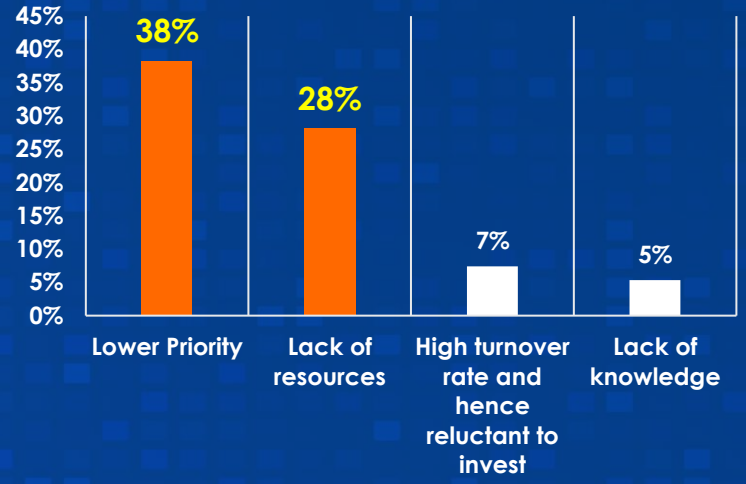


- No Regular Training
- With Regular Training

91% Retail
89% Accommodation and Catering Services
88% NGOs and Others

87% Manufacturing and Import/Export/Wholesales
85% Training and Education
75% Professional Businesses
70% Information Technology
62% Financial Services

Reason for No Regular Cybersecurity Training Provided



Overview – Internal Staff

1. Overall, **81%** businesses did not provide regular training
   - **38%** Mainly due to Low Priority
   - **28%** Lack of Resources

2. In terms of Vulnerability Level, the top 3 sectors are
   - **59%** Training and Education
   - **39%** Manufacturing and Import / Export / Wholesales
   - **39%** Retail

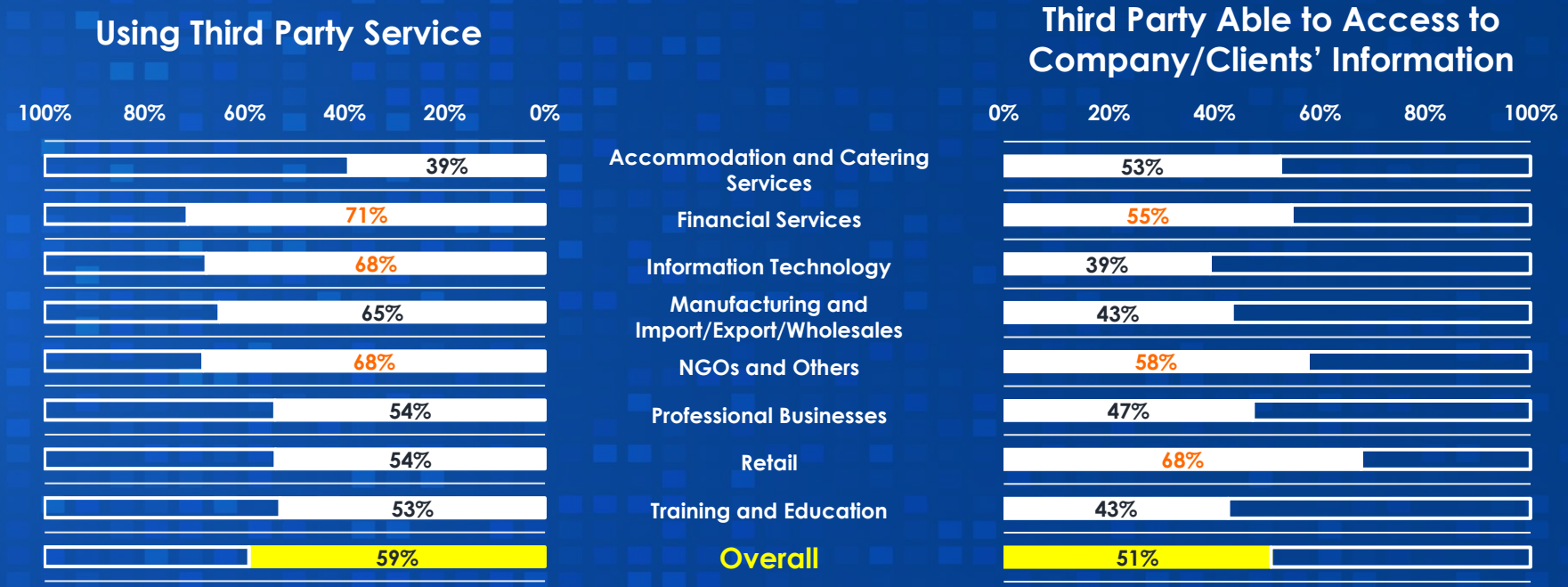
3. Although **"Retail"** is not top 3 among the 8 sectors in terms of Risk Level, due to lack of protection, the Vulnerability Level is higher

4. The Vulnerability Level of ***"Training and Education"*** is much higher than other sectors **(59%)**

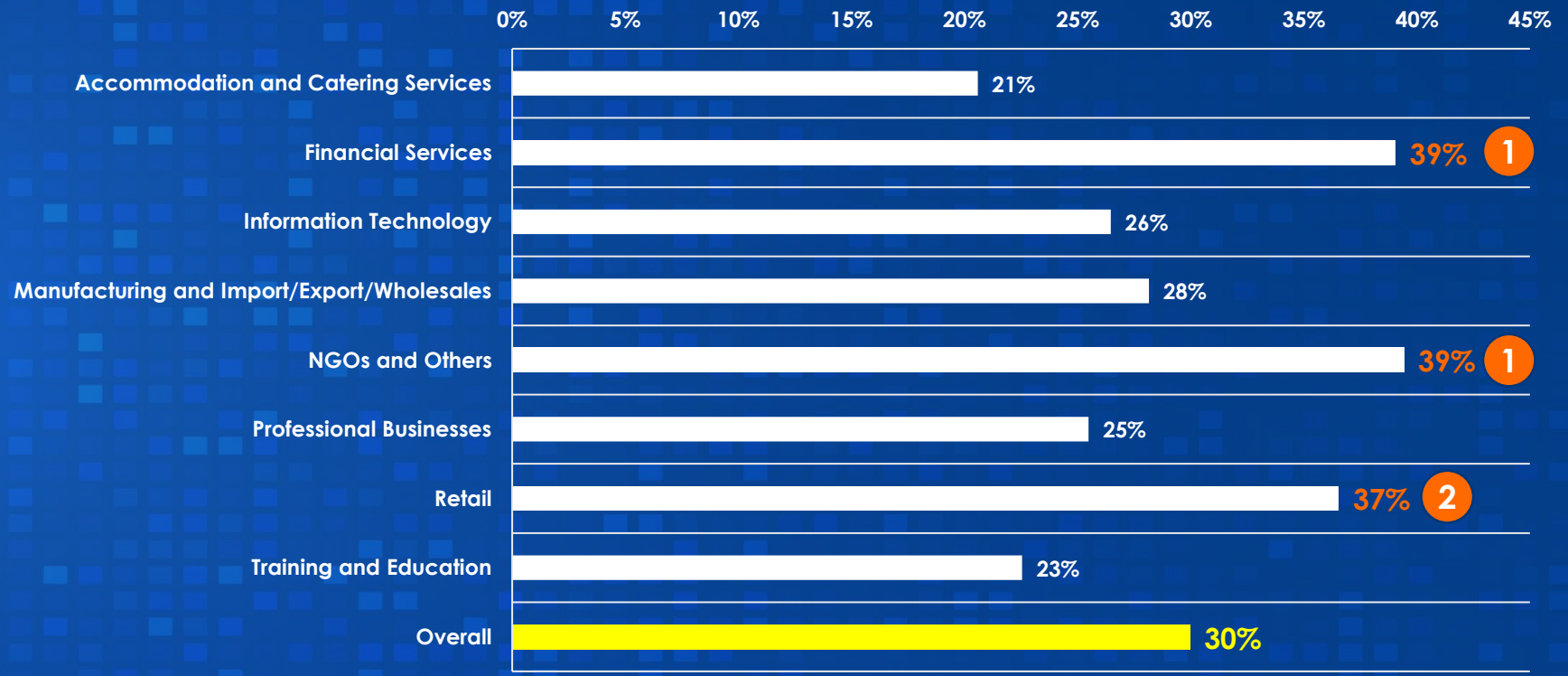
	Internal Staff Risk Level (A)	Rank	No Regular Training (B)	Rank	Vulnerability Level (A) X (B)	Rank (2)
Accommodation and Catering Services	30%	7	89%	2	27%	5
Financial Services	43%	4	62%	8	27%	6
Information Technology	27%	8	70%	7	19%	8
Manufacturing and Import/Export/Wholesales	45%	2	87%	4	39%	2
NGOs and Others	44%	3	88%	3	39%	4
Professional Businesses	35%	6	75%	6	26%	7
Retail	43%	5 (3)	91%	1	39%	3
Training and Education	69%	1	85%	5	59% (4)	1
Overall	43%		81% (1)		35%	

Supply Chain Risk

Supply Chain Risk Level

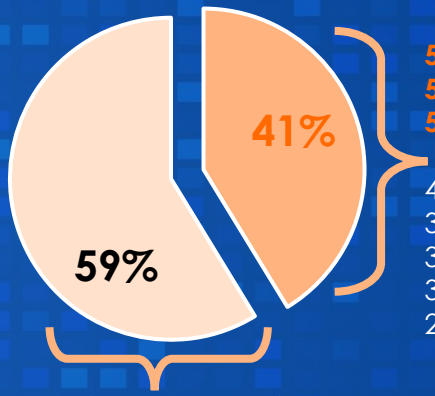


Supply Chain Risk Level



Supply Chain Risk Level

Active Protection towards Third-Party Vendor



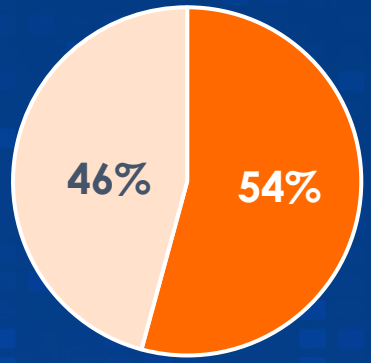
59% NGOs and Others
57% Retail
50% Accommodation and Catering Services

45% Manufacturing and Import/Export/Wholesales
39% Training and Education
35% Professional Businesses
31% Financial Services
20% Information Technology

Active protection measures include:

- **63% Restrict supplier access rights**
- **57% Encrypt for data exchange**
- **47% Regularly update software provided by suppliers**

No Active Protection Measures



Include data protection clauses in contracts with suppliers only

No Measures

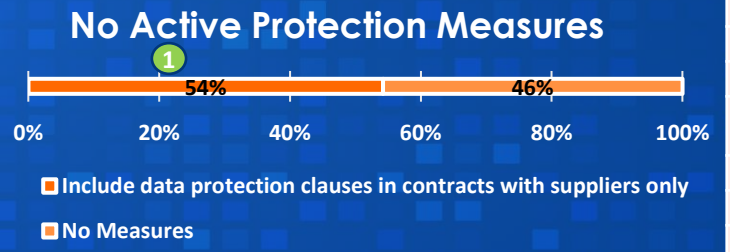
Overview – Supply Chain Risk

1. Overall, **41% no active protection**
   - Some companies **(54%)** include data protection clauses in contracts with suppliers only

2. In terms of Vulnerability Level, the top 3 sectors are
   - **23%** NGOs and Others
   - **21%** Retail
   - **13%** Manufacturing and Import/Export/Wholesales

3. Although **"Financial Service"** is top 3 in terms of Risk Level, the protection measures make it better off to reduce vulnerability level

4. **"NGOs and Others" & "Retail"** – common top 3 in both Risk Level and No Active Protection and make it the highest Vulnerability Level

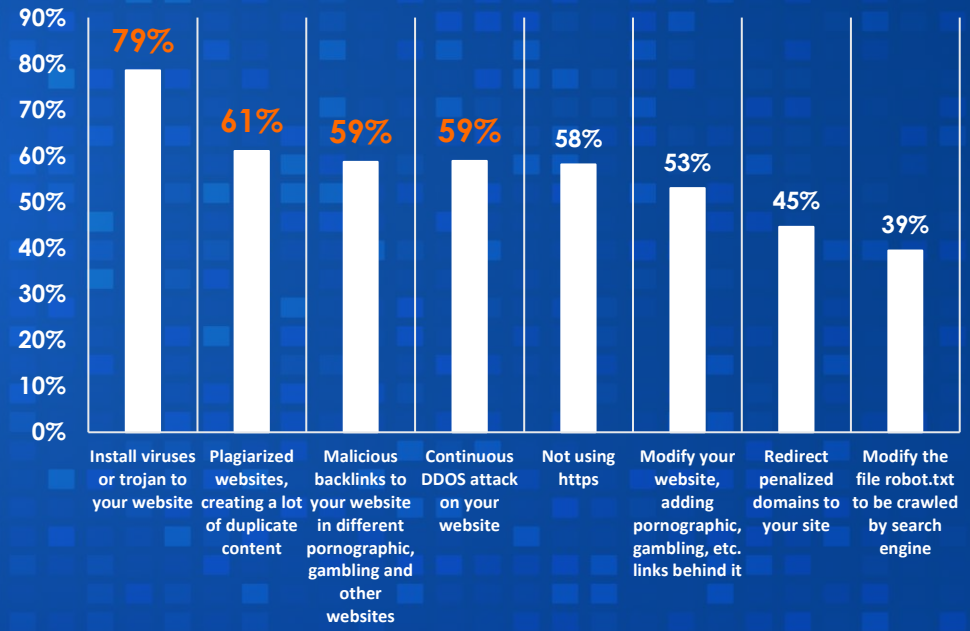


	Supply Chain Risk Level (A)	Rank	No Active Protection (B)	Rank	Vulnerability Level (A) X (B)	Rank 2
Accommodation and Catering Services	21%	8	50%	3	11%	5
Financial Services	39%	2 3	31%	7	12%	4
Information Technology	26%	5	20%	8	5%	8
Manufacturing and Import/Export/Wholesales	28%	4	45%	4	13%	3
NGOs and Others 4	39%	1	59%	1	23%	1
Professional Businesses	25%	6	35%	6	9%	7
Retail 4	37%	3	57%	2	21%	2
Training and Education	23%	7	39%	5	9%	6
Overall	**30%**		**41% 1**		**12%**	

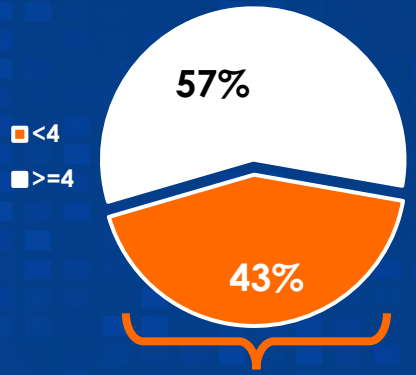
Negative SEO Risk

Negative SEO Risk Level

Awareness of the Negative Impact on SEO Ranking by Below Issues



Lack of Awareness of Negative Impact on SEO (Number of Awareness <4 Issues)

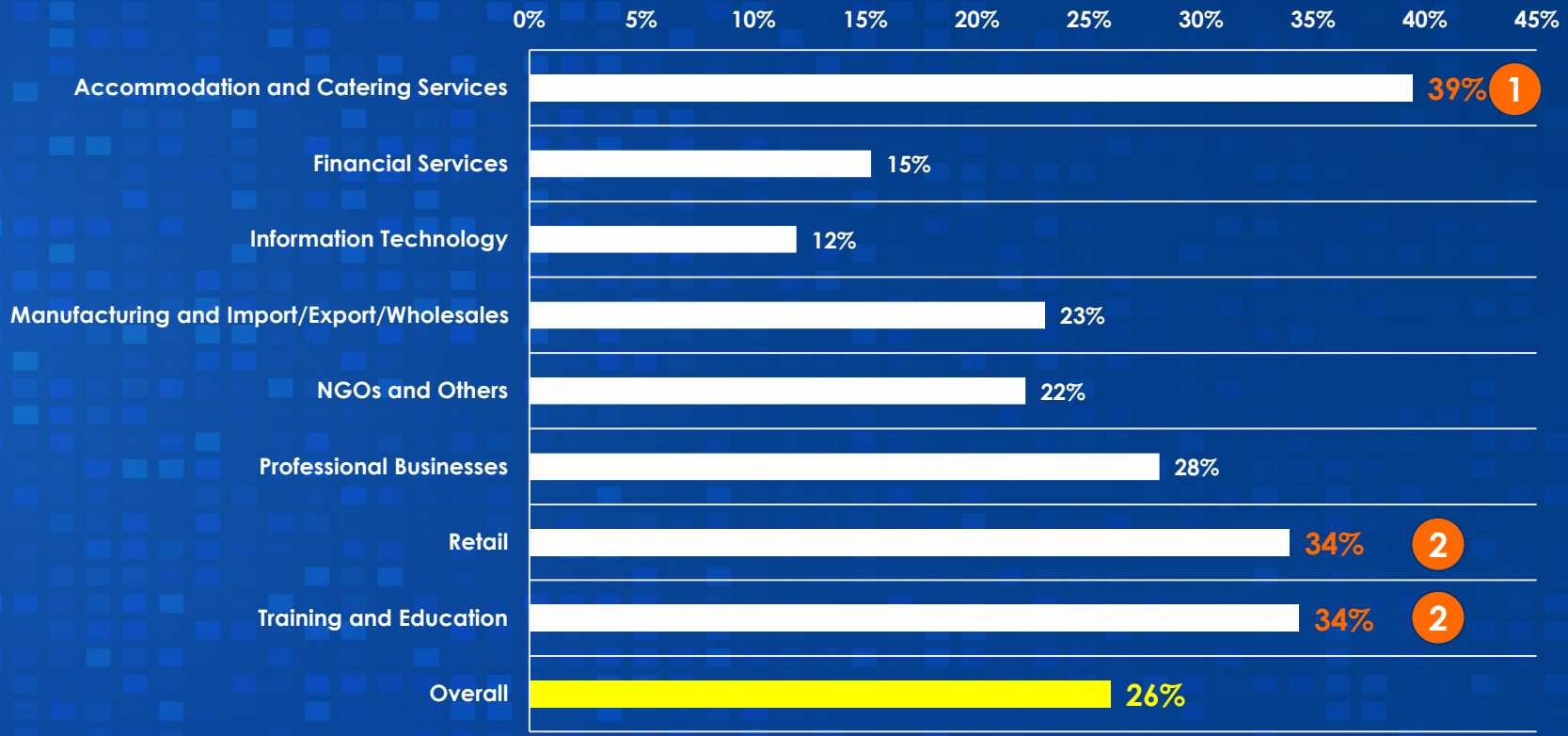


56% Accommodation and Catering Services
52% Retail
48% Training and Education

47% Professional Businesses
46% Manufacturing and Import/Export/Wholesales
45% NGOs and Others
31% Financial Services
17% Information Technology

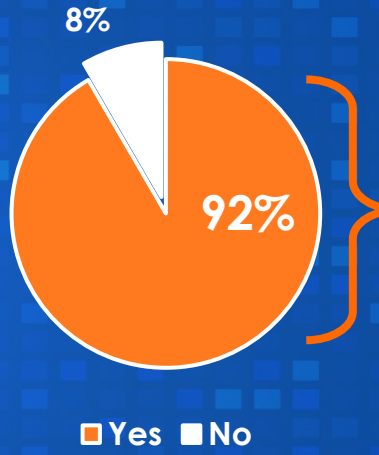
Negative SEO Risk Level

Negative SEO Risk Level

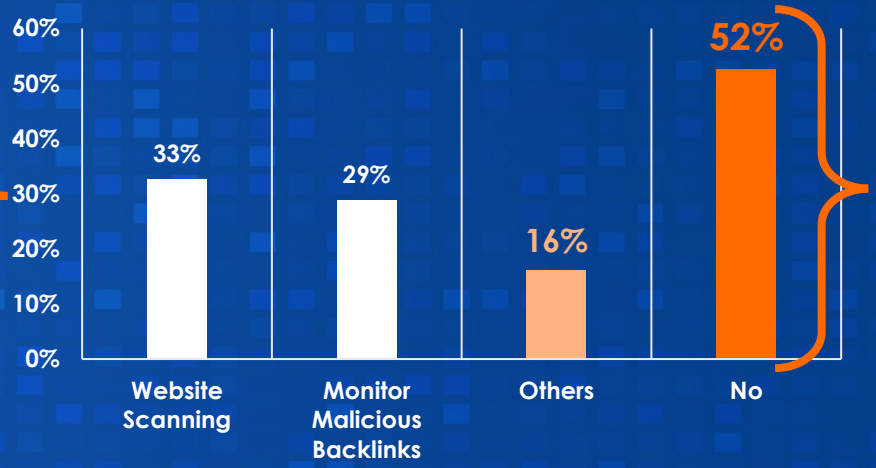


Negative SEO Risk Level

With Website



Monitor Website/ Domain



63% Manufacturing and Import/Export/Wholesales
63% Professional Businesses
63% Retail

57% Accommodation and Catering Services
55% NGOs and Others
51% Training and Education
41% Financial Services
27% Information Technology

Others include

- Monitor by firewall/ anti-virus software
- Monitor traffic (e.g. by google analytics/ backend log)
- Outsource to third-party on monitoring

Overview – Negative SEO Risk

1. Overall **52%** of business do not monitor their website/ domain to identify the risk
However some hidden risks can be only identified by regular scanning and monitoring, without being alerted by firewall/ anti-virus software

2. In terms of Vulnerability Level, the top 3 sectors are
- **22%** Accommodation and Catering Services
- **21%** Retail
- **18%** Professional Businesses

3. Although **"Professional Businesses"** is out of top 3 in terms of Risk Level, the lack of monitoring makes it Top 3 in terms of Vulnerability Level

4. Vice versa, **"Training and Education"** drops out of Top 3 due to better performance in monitoring website/domain although they are at high risk level

	Negative SEO Risk Level (A)	Rank	No Monitoring (B)	Rank	Vulnerability Level (A) X (B)	Rank (2)
Accommodation and Catering Services	39%	1	57%	4	22%	1
Financial Services	15%	7	41%	7	6%	7
Information Technology	12%	8	27%	8	3%	8
Manufacturing and Import/Export/Wholesales	23%	5	63%	2	15%	5
NGOs and Others	22%	6	55%	5	12%	6
Professional Businesses	28%	4 (3)	63%	1	18%	3
Retail	34%	3	63%	3	21%	2
Training and Education	34%	2 (4)	51%	6	18%	4
Overall	**26%**		**52%** (1)		**14%**	

Summary

Summary

1. **"Financial Services"** and **"Information Technology"** are the best-performing sectors

2. In terms of **Risk Level**, there are sector effects in different risks which make them to be **early wave of potential victim** under the emerging risks
   - **Internal Staff - Rapid digitalisation during pandemic**
   - **Supply Chain - Usage of third-party vendor**
   - **Negative SEO - Rely on online promotion**

3. "Supply Chain" – overall **lowest** vulnerability level among 3 risks

4. "Internal Staff" – **highest** in all "Vulnerability Level", "Risk Level" and "No Protection Level" **despite the highest awareness level (72%) as shown in P.4** (知易行難)

5. Although its business nature make it at high risk, the vulnerability level can be effectively **reduced with protection**,
e.g "Financial Services" in Supply Chain

6. **"Retail"** is top 3 in terms of Vulnerability Level among all 3 risks

	Internal Staff Risk Level (2)	No Regular Training	Vulnerability Level	Supply Chain Risk Level (2)	No Active Protection	Vulnerability Level (2)	Negative SEO Risk Level	No Monitoring	Vulnerability Level
Accommodation and Catering Services	30%	89%	27%	21%	50%	11%	39%	57%	22%
Financial Services (1)	43%	62%	27%	39%	31%	12% (5)	15%	41%	6%
Information Technology (1)	27%	70%	19%	26%	20%	5%	12%	27%	3%
Manufacturing and Import/Export/Wholesales	45%	87%	39%	28%	45%	13%	23%	63%	15%
NGOs and Others	44%	88%	39%	39%	59%	23%	22%	55%	12%
Professional Businesses	35%	75%	26%	25%	35%	9%	28%	63%	18%
Retail (6)	43%	91%	39%	37%	57%	21%	34%	63%	21%
Training and Education	69%	85%	59%	23%	39%	9%	34%	51%	18%
Overall	**43%**	**81% (4)**	**35%**	**30%**	**41%**	**12% (3)**	**26%**	**52%**	**14%**

Advice from HKIRC

Internal Staff Risk

- ✓ Provide **regular training**, leverage free resources if any difficulties
- ✓ Conduct phishing drill as **assessment**
- ✓ Subscribe to **daily cybersecurity news** to understand the latest industry trend, both locally and globally

Supply Chain Risk

- ✓ Not only data protection clauses to transfer responsibility, but also **active protection measures.** Ultimately the damage will also affect your company if it happens
- ✓ Active protection measures to consider
  - Conduct **security assessment** to vendors during appointment or renewal
  - Set **access control** with vendors
  - **Encrypt** data transaction with vendors
  - **Install regular software updates** from vendors
  - **Remove unnecessary access immediately** once task/service completed

Negative SEO Risk

- ✓ Understand what the **common negative SEO issues** are(e.g. the 8 issues covered in P.16)
- ✓ Conduct **regular website scanning**
- ✓ Conduct **regular backlink monitoring**
- ✓ Apply SSL certificate for **https** website
- ✓ **Report** to search engine service provider once malicious findings are sought

Advice from HKIRC – Free Resources

HKIRC Cybersec Training Hub

- Free platform for staff's cybersecurity awareness training
- E-certificate will be generated for staff management upon completion

Website: https://cyberhub.hk

Cybersec Infohub

- Cybersecurity information shared by industry experts
- Receive daily cybersecurity news
- Raise questions to security experts
- Regular cybersecurity events

Website: https://cybersechub.hk

Free Webscan Service to .hk Users

- Free website security scanning service
- Free consultation services

Website: https://hkirc.hk

CyberDefender

- Security checking tools, e.g. password strength/ Phishing Scam Search Engine
- Cybersecurity events and programmes

Website: https://cyberdefender.hk/

Cyber Security Information Portal

- Security Advice
- Best Practices

Website: https://www.cybersecurity.hk/

Thank You