CYBERSEC 2024
臺灣資安大會
5/14 Tue – 5/16 Thu
臺北南港展覽二館
Generative Future

上市櫃資安標竿論壇

企業如何應對美國證交委員會 SEC 新資安規定

李彥民 Anthony

CISO 資安長

LinkedIn: Anthony3000

先來個冷笑話鋪梗

有一個資安長花了很多時間替公司做了很多資安威脅分析，最後終於釐清了兩個最大的威脅，猜猜看是哪兩種人?

答案:

2. 公司內部的人

1. 公司外部的人

SEC 2023年 新資安規定條文

Generative Future

	項目	主題	要求說明
1	Form 10-K - Regulation S-K Item 106(b)	Risk management, and Strategy 風險管理與策略	Registrants **must** - describe their processes, if any, for the assessment, identification, and management of **material risks** from cybersecurity threats, and - describe whether any risks from cybersecurity threats have materialy affected or are reasonably likely to **materially** affect their **business strategy, results of operations, or financial condition**.
2	Form 10-K - Regulation S-K Item 106(c)	Governance 治理	Registrants **must:** - Describe the board's oversight of risks from cybersecurity threats - Describe management's role in assessing
3	Form 8-K Item 1.05	Material Cybersecurity Incidents 實質重大的事故	**Registrants must disclose any cybersecurity incident they experience that is determined to be material**, and describe the material aspects of its: - Nature, scope, and timing; and - Impact or reasonably likely impact. - An Item 1.05 Form 8-K must be filed with **four business days of determining an incident was material**. A registrant may delay filling as described below, if the United States Attorney General("Attorney General") determines immediate disclosure would pose a substantial risk to national security or public saftety. Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was
4	Form 20-F	FPI – Risk Management, Strategy and Governance	Foreign Private Issuers **must**: - Describe the board's oversight of risks from cybersecurity threats. - Describe management's role in assessing and managing **material risks** from cybersecurity threats
5	Form 6-K	FPI – Material Cybersecurity Incident	FPIs **must** furnish on Form 6-K information on **material** cybersecurity incidents that they disclose or otherwise publicize in a foreign juridiction, to any stock exchange, or to security holders

Reference: sec

美國證交委員會規則要求重點

What is "Material"?
Supreme Court has deemed material information: a fact is material if there is a "substantial likelihood that a reasonable investor would consider it important" or if it would have "significantly altered the 'total mix' of information made available."

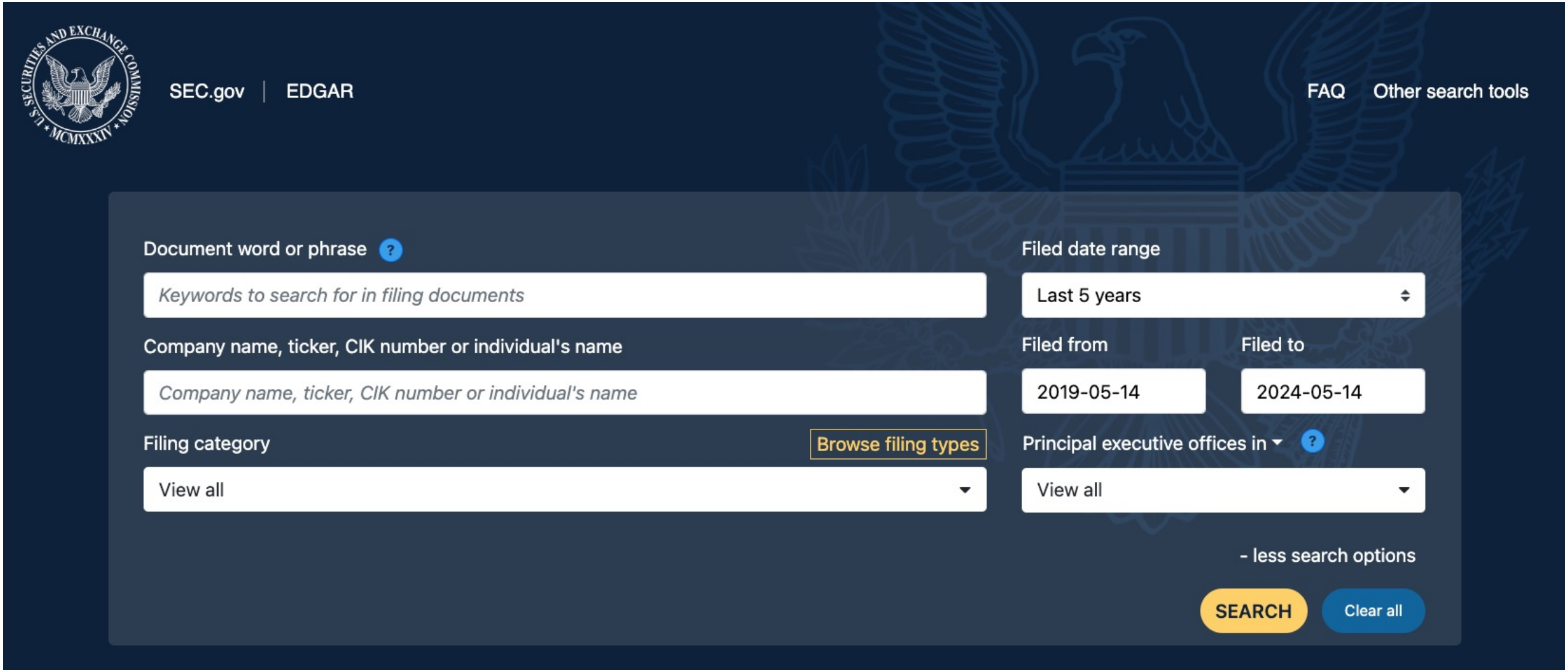
什麼是 "Material"? 材料? 事實? 實值的，重要的，重大的!
[ChatGPT翻譯] 引用美國最高法院的定義： 若有「合理投資者會認為其重要的重大可能性」或「明顯改變已提供信息的整體組合」的情況，該事實即為重要。

[我的翻譯]
1. 投資者有很高的機率會認為是重大事件
2. 所揭露的資安事件會改變整體公司經營狀況

FAIR-MAM (實質評估模型)= 實值的損失是用「錢」來表示

Reference: pwc, cambridge

https://www.sec.gov/edgar/search/#



Reference: sec,

The Clorox Company 8-K Aug 2023

Generative Future

Item 8.01 Other Events.

On Aug. 14, 2023, The Clorox Company (the "Company" or "Clorox") announced that it had identified unauthorized activity on some of its Information Technology (IT) systems and took immediate steps to stop and remediate the activity, including taking certain systems offline. The Company implemented its business continuity plans and began manual ordering and processing procedures shortly thereafter at a reduced rate of operations. The Company is operating at a lower rate of order processing and has recently begun to experience an elevated level of consumer product availability issues.

Based on the information available to date, the Company believes the unauthorized activity is contained due to the steps the Company has taken to add

The cybersecurity attack damaged portions of the Company's IT infrastructure, which caused widescale disruption of Clorox's operations. Th actively taken offline. The Company expects to begin the process of transitioning back to normal automated order processing the week of Sept. 25. Clorox has al up to full production to occur over time. At this time, the Company cannot estimate how long it will take to resume fully normalized operations.

Clorox is still evaluating the extent of the financial and business impact. Due to the order processing delays and elevated level of produc mature for the Company to determine longer-term impact, including fiscal year outlook, given the ongoing recovery.

The Company will provide an update as to financial impact after it has increased visibility.

資安事件損失 0.35 ~ 0.75 每股

Reconciliation of Preliminary Adjusted Earnings (Losses) Per Share Information
(Dollars in millions except per share data)

	Three Months Ended Sept. 30, 2023 (Preliminary estimated range)	
	Diluted Earnings (Losses) Per Share	
	Low	High
As estimated (GAAP)	$ (0.75)	$ (0.35)
Cybersecurity attack costs [1]	0.14	0.14
Streamlined operating model [2]	0.02	0.02
Digital capabilities and productivity enhancements investment [3]	0.19	0.19
As adjusted (Non-GAAP)	$ (0.40)	$ (0.00)

(1) During the three months ended Sept. 30, 2023, the Company expects to incur approximately $25 ($19 after tax) of costs related to the cybersecurity attack. These costs relate to third-party consulting services, including forensic experts, legal counsel and other IT professional services, as well as incremental operating costs incurred from the resulting disruption to parts of the Company's business operations.

(2) During the three months ended Sept. 30, 2023, the Company expects to incur $3 ($2 after tax) of restructuring and related costs, net related to implementation of the streamlined operating model.

(3) During the three months ended Sept. 30, 2023, the Company expects to incur approximately $32 ($24 after tax) of operating expenses related to its digital capabilities and productivity enhancements investment.

Reference: sec,

23andMe Holding Co. 8-K Oct 2023

Item 7.01 Regulation FD Disclosure

On October 10, 2023, 23andMe Holding Co. (the "Company," "23andMe," "we," "us," and "our") filed a Current Report on Form 8-K (the "Original Form 8-K") reporting that it learned that certain user profile information, which a 23andMe user (each, a "user" and collectively, the "users") creates and chooses to share with their genetic relatives in 23andMe's DNA Relatives feature, was accessed and downloaded from individual 23andMe.com (the "23andMe website") user accounts (the "incident") by a threat actor (the "threat actor"). The Company is filing this Amendment No. 1 to the Original Form 8-K (this "Amendment") to provide supplemental information regarding the incident. Except as expressly set forth herein, this Amendment does not amend the Original Form 8-K in any way and does not modify or update any other disclosures contained in the Original Form 8-K. This Amendment supplements the Original Form 8-K and should be read in conjunction with the Original Form 8-K.

On October 1, 2023, a threat actor posted online a claim to have 23andMe users' profile information. Upon learning of the incident, 23andM
immediately commenced an investigation and engaged third-party incident response experts to assist in determining the extent of any un
activity. Based on its investigation, 23andMe has determined that the threat actor was able to access a very small percentage (0.1%) of
instances where usernames and passwords that were used on the 23andMe website were the same as those used on other websites tha
previously compromised or were otherwise available (the "Credential Stuffed Accounts"). The information accessed by the threat ac
Stuffed Accounts varied by user account, and generally included ancestry information, and, for a subset of those accounts, health-re
based upon the user's genetics. Using this access to the Credential Stuffed Accounts, the threat actor also accessed a significant num
containing profile information about other users' ancestry that such users chose to share when opting in to 23andMe's DNA Relatives
certain information online. We are working to remove this information from the public domain. As of the filing date of this Amendme
believes that the threat actor activity is contained.

23andMe is in the process of providing notification to users impacted by the incident as required by applicable law. While no company can ever
completely eliminate the risk of a cyber attack, the Company has taken certain steps to further protect its users' data. For example, on October 10, 202
23andMe required all users to reset their passwords, and on November 6, 2023, 23andMe required all new and existing users to login into the 23andM
website using two-step verification going forward.

As of the filing date of this Amendment, the Company expects to incur between $1 million and $2 million in onetime expenses related to the incident during its fiscal third quarter ending December 31, 2023, primarily consisting of technology consulting services, legal fees, and expenses of other third-party advisors. The Company believes that such expenses and the direct or indirect business impacts of the incident could negatively affect its financial results. As of the filing date of this Amendment, the Company is not able to predict whether such direct or indirect impacts of the incident could have a material effect on its financial condition and/or results of operations for the fiscal year ending March 31, 2024.

As of the filing date of this Amendment and as a result of the incident, multiple class action claims have been filed against the Company in federal and state court in California and state court in Illinois, as well as in British Columbia and Ontario, Canada, which the Company is defending. These cases are at an early stage, and the Company cannot predict the outcome. The Company is also assessing its response to notices filed by consumers under the California Consumer Privacy Act and to inquiries from various governmental officials and agencies. The full scope of the costs and related impacts of this incident and related litigation, including, without limitation, the availability of insurance to offset some of these costs, cannot be estimated at this time.

While the Company believes the investigation into these matters is complete, the Company may become aware of new or different information or information that differs from that contained in this Current Report on Form 8-K. All information provided in this Amendment is as of the date hereof and 23andMe's undertakes no duty to update this information except as required by applicable law.

資安事件損失 1~2百萬元

Reference: sec,

Okta 8-K Nov 2023

Generative Future

Forward-Looking Statements: This press release contains "forward-looking statements" within the meaning of the "safe harbor" provisions of the Private Securities Litigation Reform Act of 1995, including but not limited to, statements regarding our financial outlook, business strategy and plans, market trends and market size, opportunities and positioning. These forward-looking statements are based on current expectations, estimates, forecasts and projections. Words such as "expect," "anticipate," "should," "believe," "hope," "target," "project," "goals," "estimate," "potential," "predict," "may," "will," "might," "could," "intend," "shall" and variations of these terms and similar expressions are intended to identify these forward-looking statements, although not all forward-looking statements contain these identifying words. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond our control. For example, the market for our products may develop more slowly than expected or than it has in the past; there may be significant fluctuations in our results of operations and cash flows related to our revenue recognition or otherwise; we may not achieve expected synergies and efficiencies of operations between Okta and Auth0, and we may not be able to successfully integrate the companies; global economic conditions could worsen; a prior or future network, data or cybersecurity incident that has allowed or does allow unauthorized access to our network or data or our customers' data could damage our reputation, cause us to incur significant costs or impact the timing or our ability to land new customers or retain existing customers; we could experience interruptions or performance problems associated with our technology, including a service outage; and we may not be able to pay off our convertible senior notes when due. Further information on potential factors that could affect our financial results is included [illegible] and our other filings with the Securities and Exchange Commission. The forward-looking statements included in this pre[illegible]s release and we assume no obligation and do not intend to update these forward-looking statements.

1. 失去現有客戶與未來新客戶 (生產力損失)
2. 可能的聲譽損失
3. 事件應變損失

Reference: sec, okta

能力要求重點(要做什麼？)

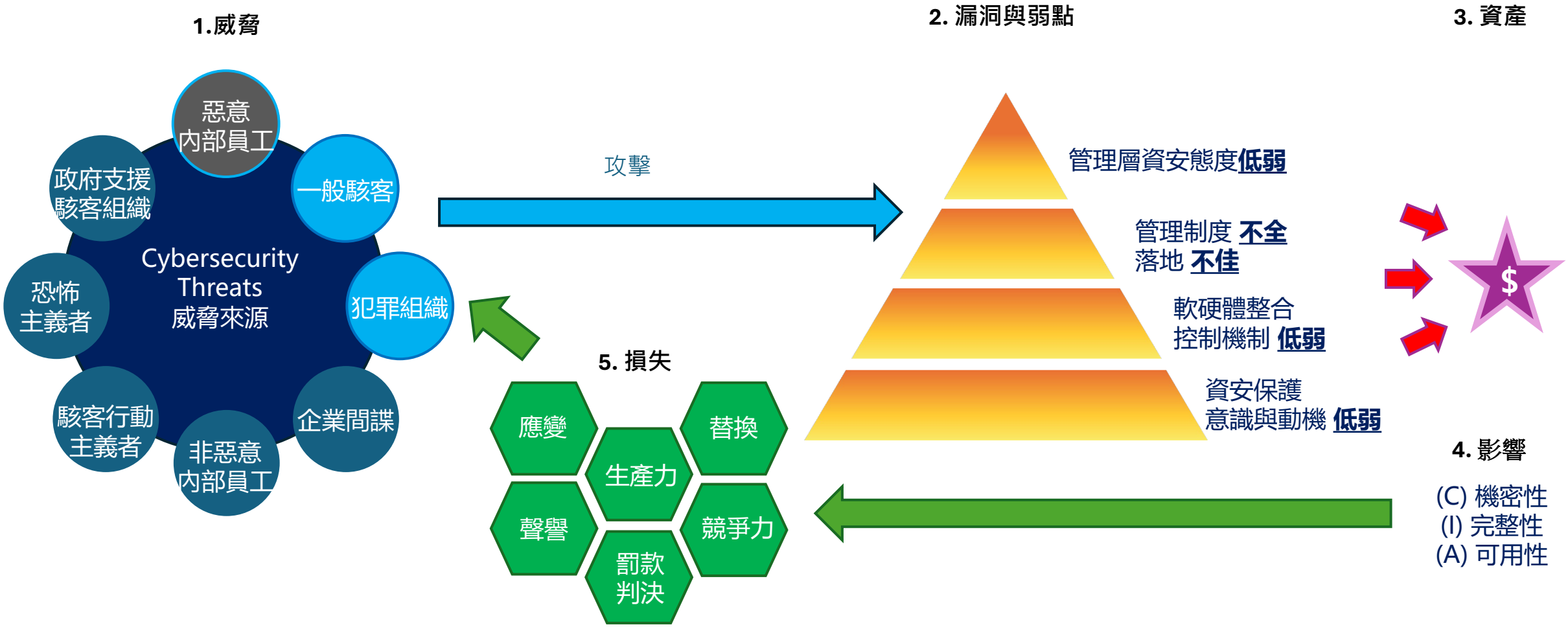
1. 資安風險管理與策略 Cyber Risk Management & Strategy
    1) Drive accountability over cyber posture into the business
    2) Embed risks and controls in process technology, **measure** and monitor
    3) Extensive leadership reporting of cyber program effectiveness and cyber posture

2. 資安治理 Cyber Governance
    1) Formalize disclosure statements to be included in the 10-K and continue to enhance them as the cybersecurity program is enhanced.
    2) **Further incorporate cyber security risk into financial planning** and **capital investments**
    3) Execute board oversight with robust reporting of cyber program effective-ness and cyber posture and continual upskilling/access to expertise

3. 資安事件應變通知 Cyber Incident Reporting
    1) Enhance processes and procedures to meet 4 day disclose **material** cyber incident requirements
    2) Develop processes to manage multiple compliance disclosure requirements
    3) Develop processes to evaluate whether past incidents are related and require aggregation

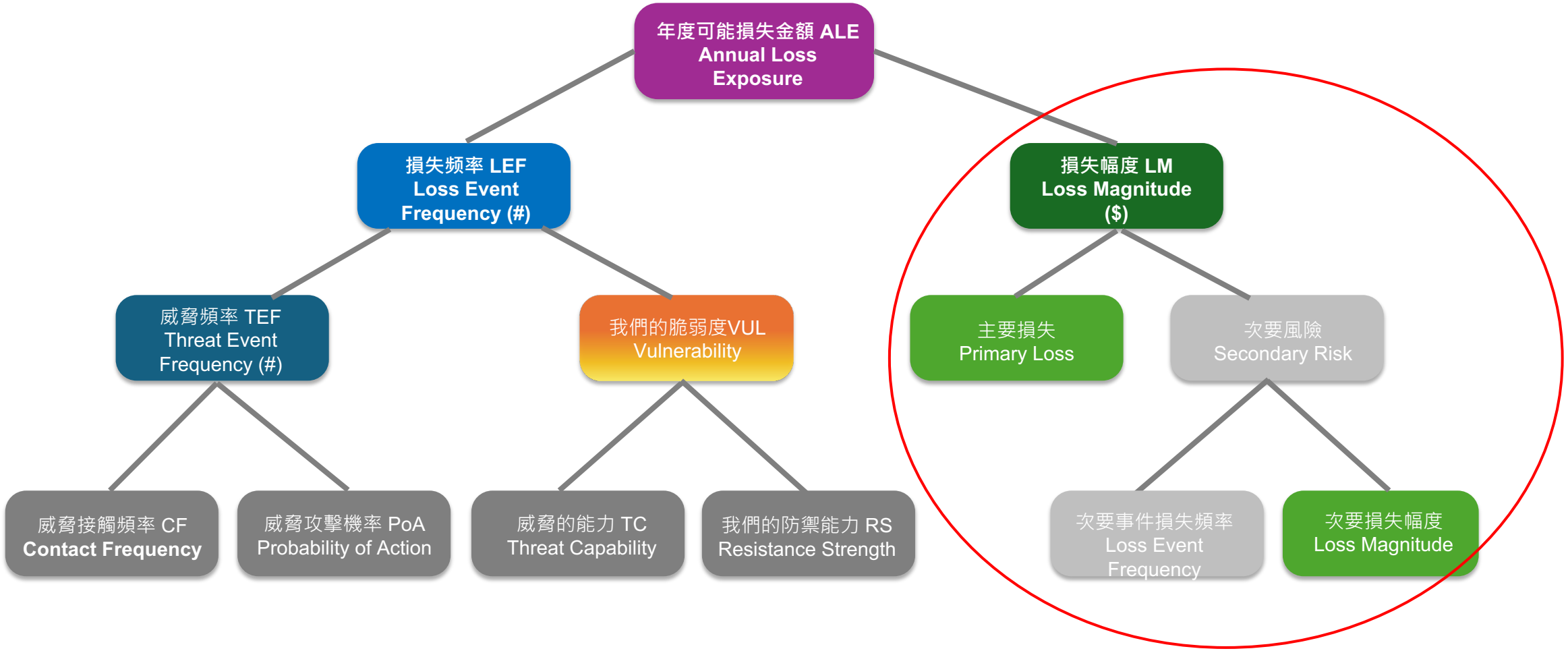
Reference: pwc,

五大元素：威脅，弱點，資產，影響與損失



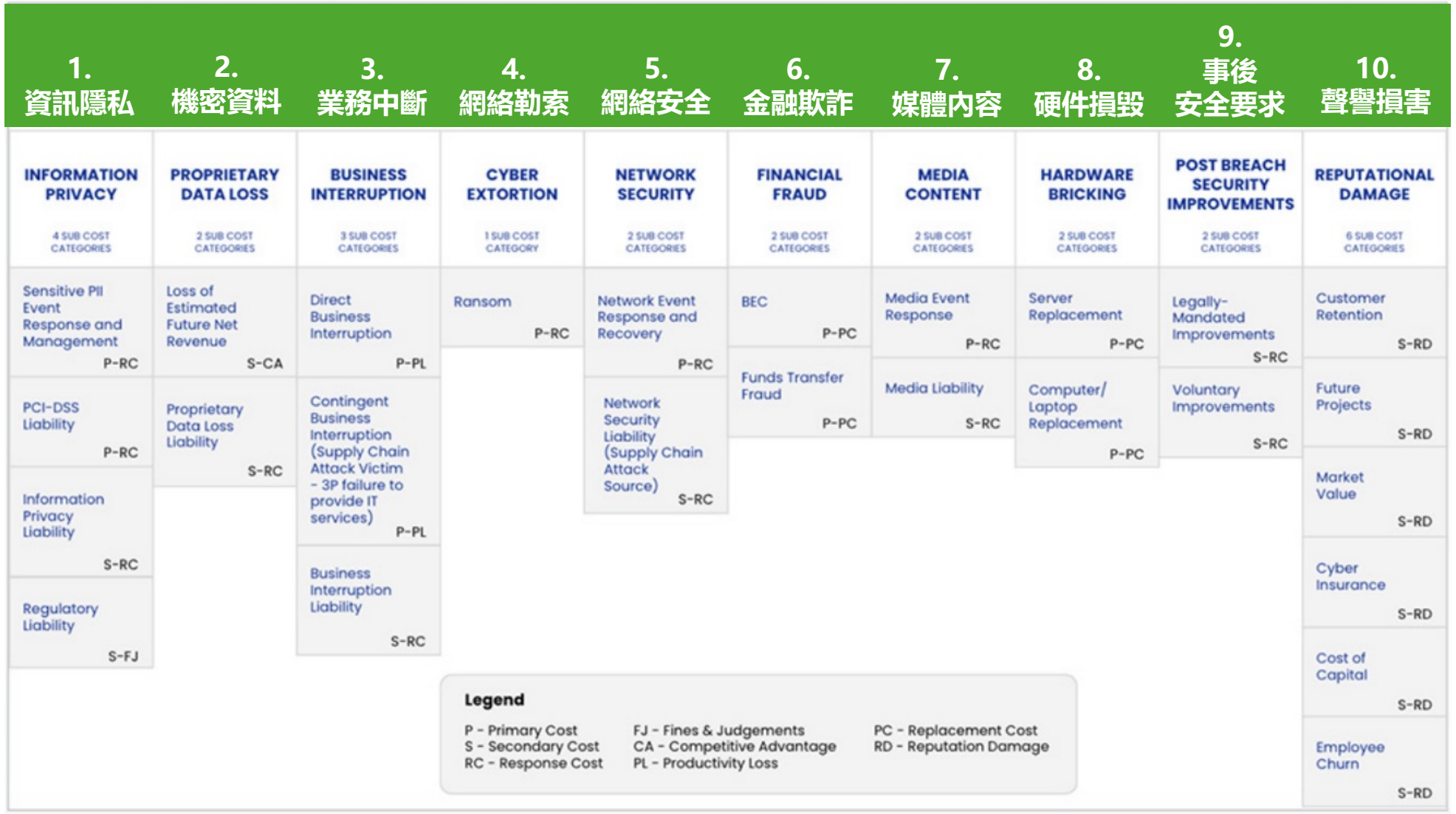
Reference: FAIR,

FAIR 風險量化模型



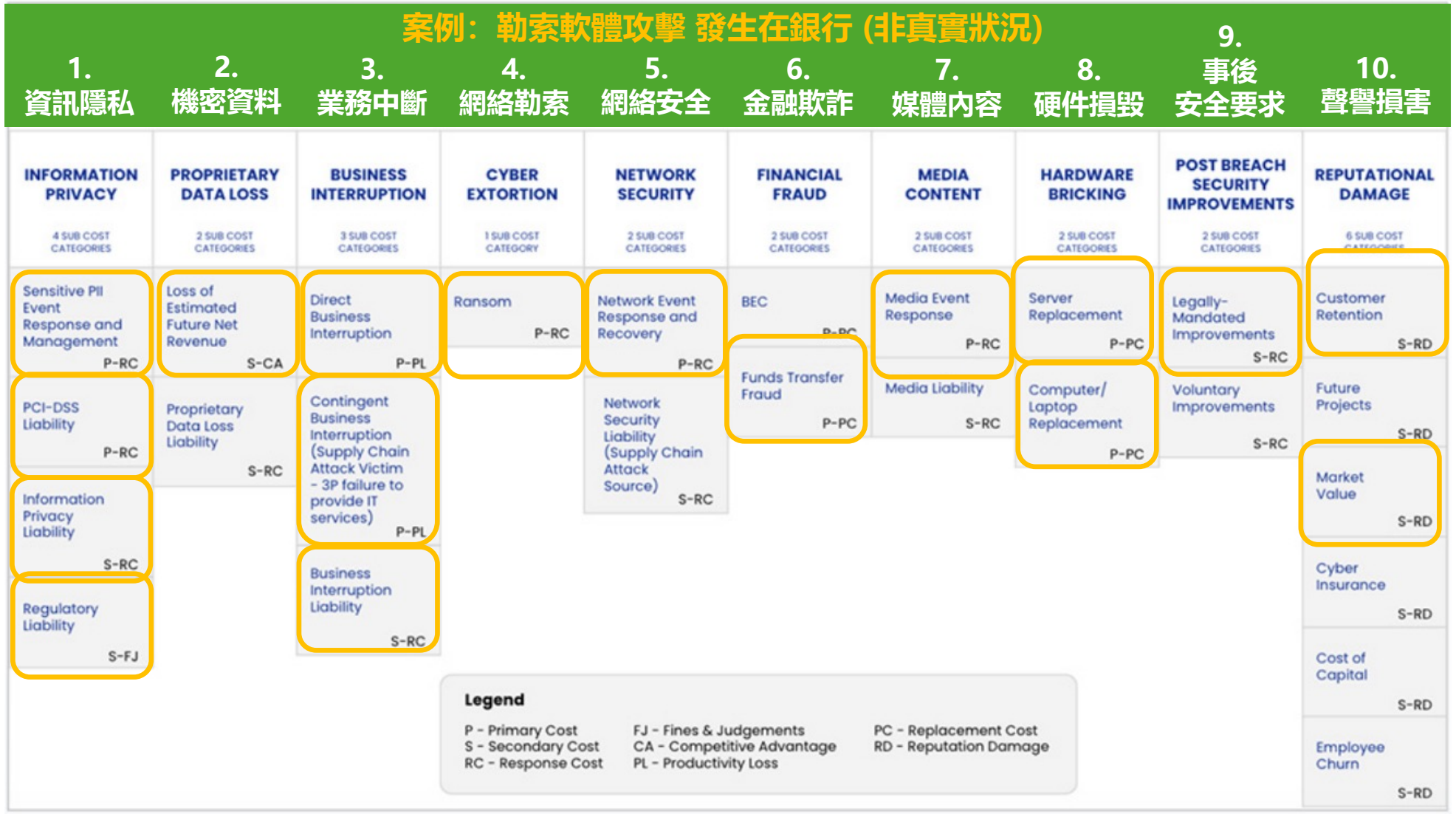
Reference: FAIR,

FAIR-MAM 網路攻擊成本模型



Referance: FAIR-MAM™

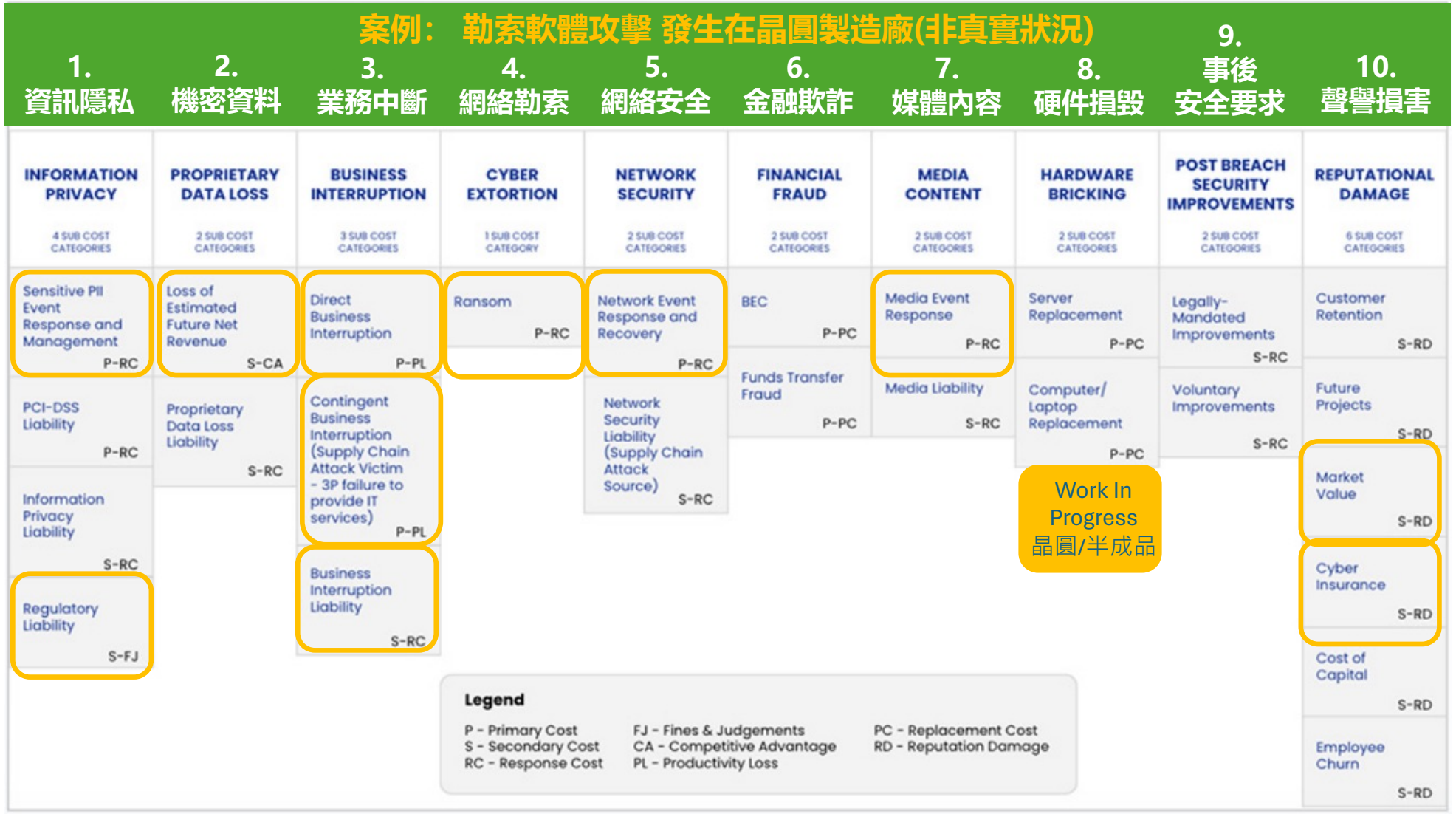
FAIR-MAM 網路攻擊成本模型



Referance: FAIR-MAM™

FAIR-MAM 網路攻擊成本模型

Generative Future



Referance: FAIR-MAM™

最後一個笑話

事件發生後，
要能四天內快速的盤點
「實質的損失」大概是多少錢？

再來一些哲學題功課

假如一棵樹在森林裡倒下而沒有人在附近聽見，它有沒有發出聲音?
If a tree falls in a forest and no one is around to hear it, does it make a sound?

1. 假如攻擊沒有任何造成金錢的損失，那是還是風險嗎?
2. 假如攻擊機率是每年0.000001次，那還需要擔心那個風險嗎？要用多少資源防禦它?
3. 假如駭客沒有攻擊你的動機，那還需要擔心那個風險嗎?
4. 假如你的資產沒有價值，那還需要擔心被攻擊的風險嗎?
5. 假如你的資產價值定義是「高」，但是市場的評估工具認為找到的漏洞風險「小」，所以不用處理?

Thank you

LinkedIn: Anthony3000