RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **SAO-W06V**

Getting the Security and Flexibility Balance Right in a COVID-19 World

Magda Lilia Chelly

Head of Cyber Consulting, Former CISO, Entrepreneur
CISSP, S-CISO, PhD.
Marsh Asia
@m49D4ch3lly

COVID19 Threats

For Employees	For Companies
Working remotely, with access to enterprise apps at any time	Increased reliance on service providers and third parties to assist in transition to remote work
Increased use of personal devices that are not “company-issued”, growing “**Shadow IT**” risks	**Increased variability and uncertainty leading to lack of visibility on emerging cyber risks**
Connecting through **home router / Wi-Fi** systems without advanced security capabilities	Cybercriminals exploiting **COVID-19 panic** to launch new phishing campaigns
Inability perform security tasks, creating challenges with real time monitoring and Security Operations Services (SOC)	Fake social media profiles / users disseminating disinformation

COVID19 Threats

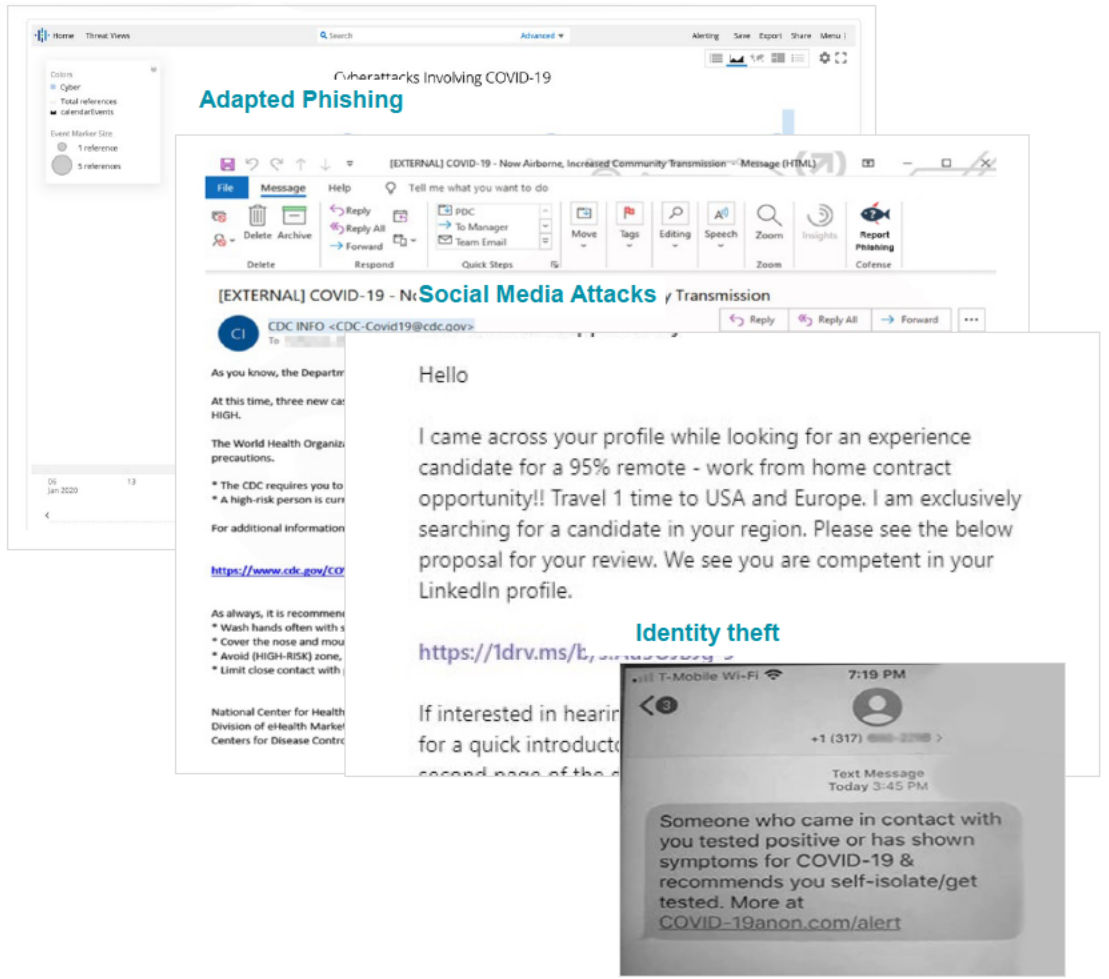
Phishing: Malicious links, claiming important news updates on the virus, targeting both personal and work emails

Domain Names: **COVID-19**-related domain names (up to nearly 800 per day in early March), including domains like “cdc[.]gov” and “who[.]int”

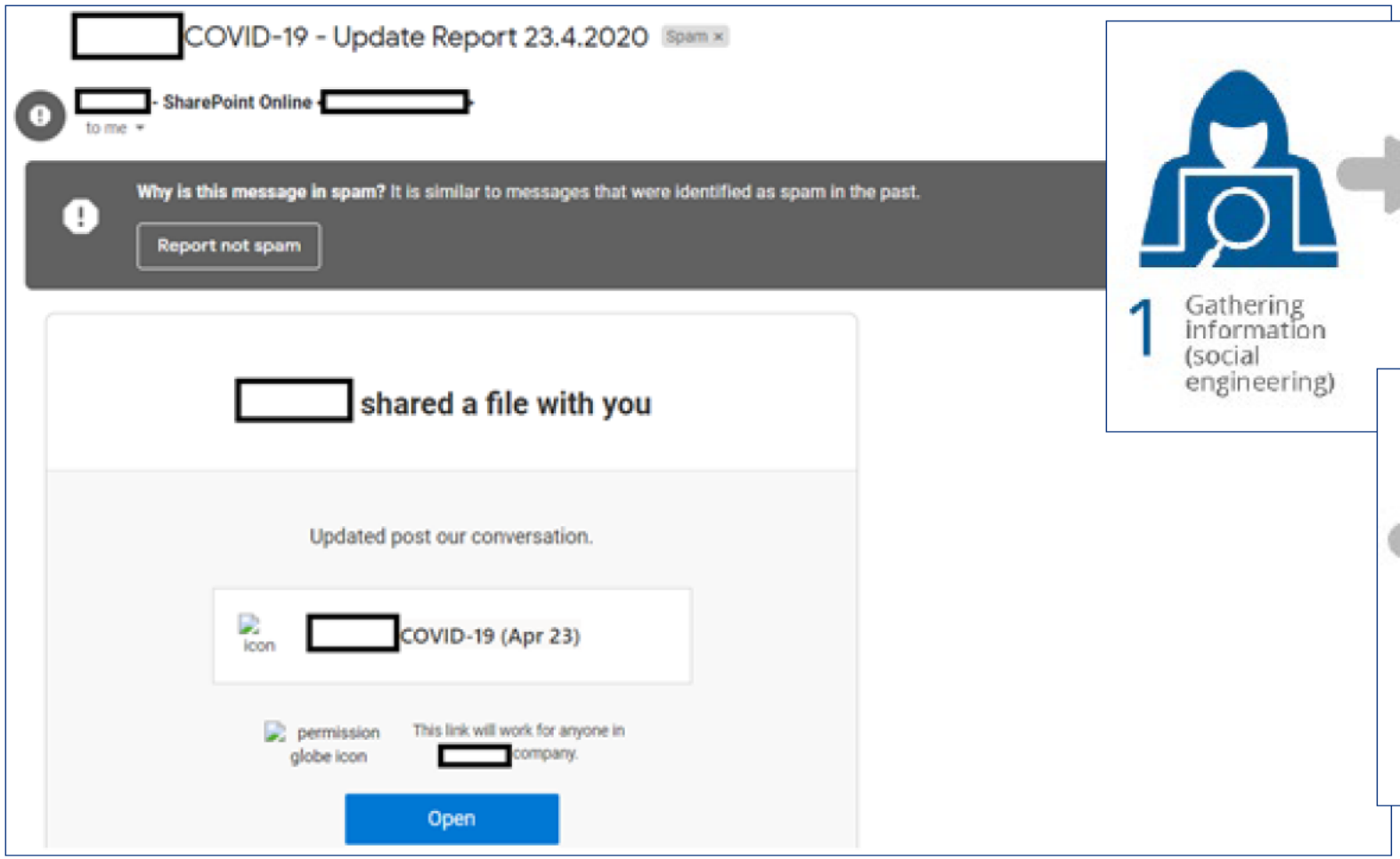
Social Media: Fake accounts are spreading disinformation through additional channels, running malware, i.e. ransomware, credential theft, or fraud

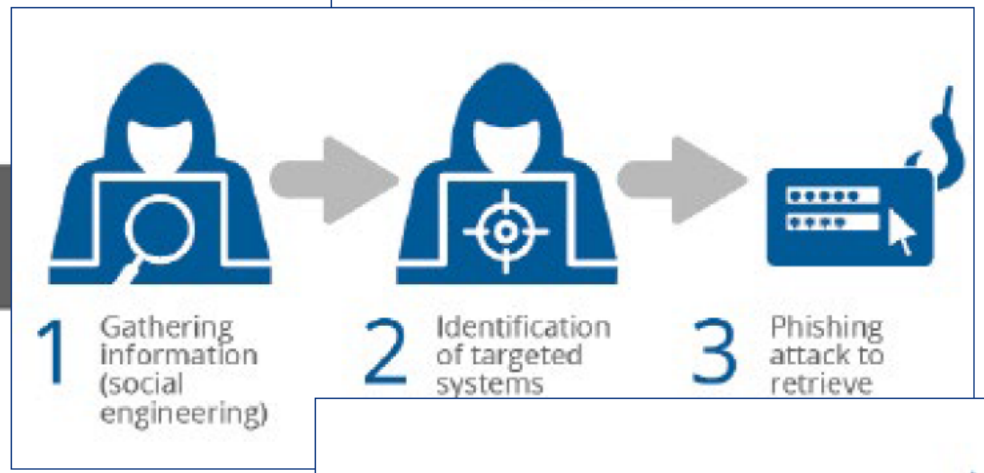
Phone / Voice: Increasingly advanced voice and video technology attacks are used to commit fraud and infiltrate enterprise systems

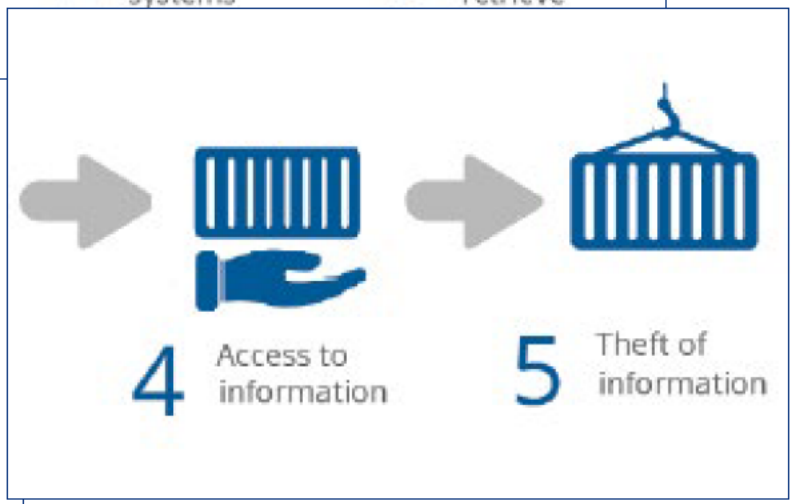
Threat landscape – extract from Recorded Future



A COVID19-themed Phishing Attack Could Lead to Data Theft or Business Interruption (i.e. ransomware attack)







Losses from cyberattacks can be significant

including compensations to impacted customers, business interruptions, or reputational damage

Business
"What is our cyber exposure and cyber risks?"

CISO
"What cyber initiative should I prioritize?"

IT Manager or CIO
"I have a firewall, why do I need more security?"

CRO
"What cyber insurance do we need?"

CEO
"What is my expected financial loss in case of cyber event?"

Board
"What is our ROI for cyber security expenses ?

CFO
"How do we optimize our cyber security spending?"

A majority of organizations in 2019 are spending **8-12% of their IT budget on cybersecurity**, however

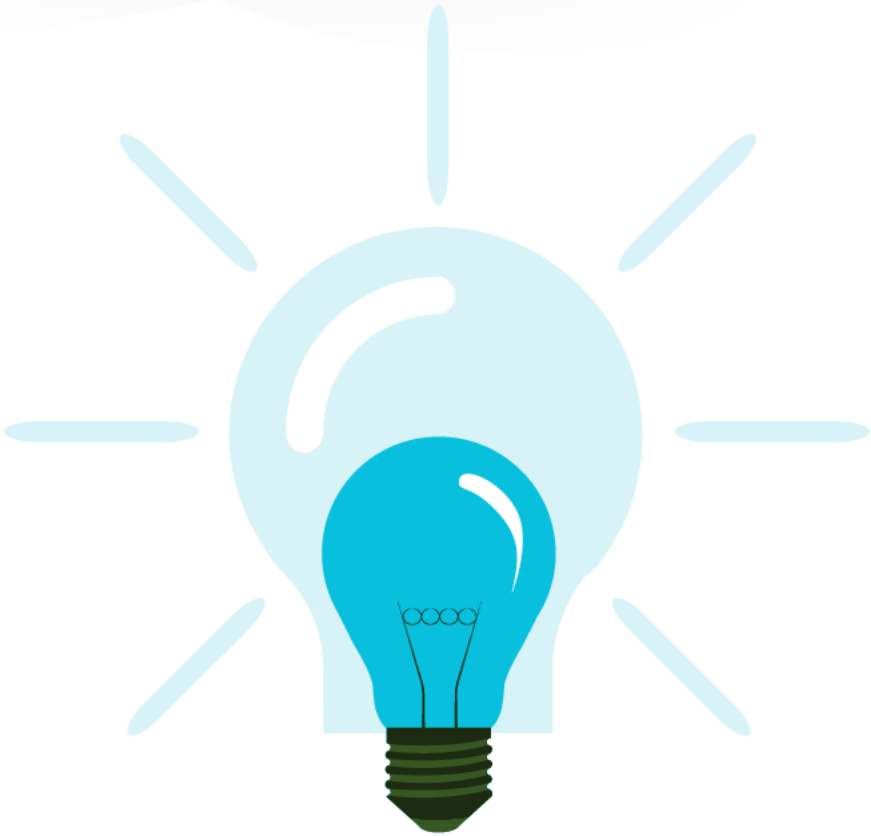
70%

were not expressing **their cyber risk exposures** to drive investment decisions in cyber security.

Source: https://www.forbes.com/sites/forbestechcouncil/2019/05/09/yes-virginia-you-can-calculate-roi-for-cybersecurity-budgets/#78dde9a63ad4https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

Traditional Security Does Not Work Anymore …

- Translate cyber risk into **business risk** with risk quantification;
- Deliver a continuous cyber risk assessment;
- Combine **security & usability**

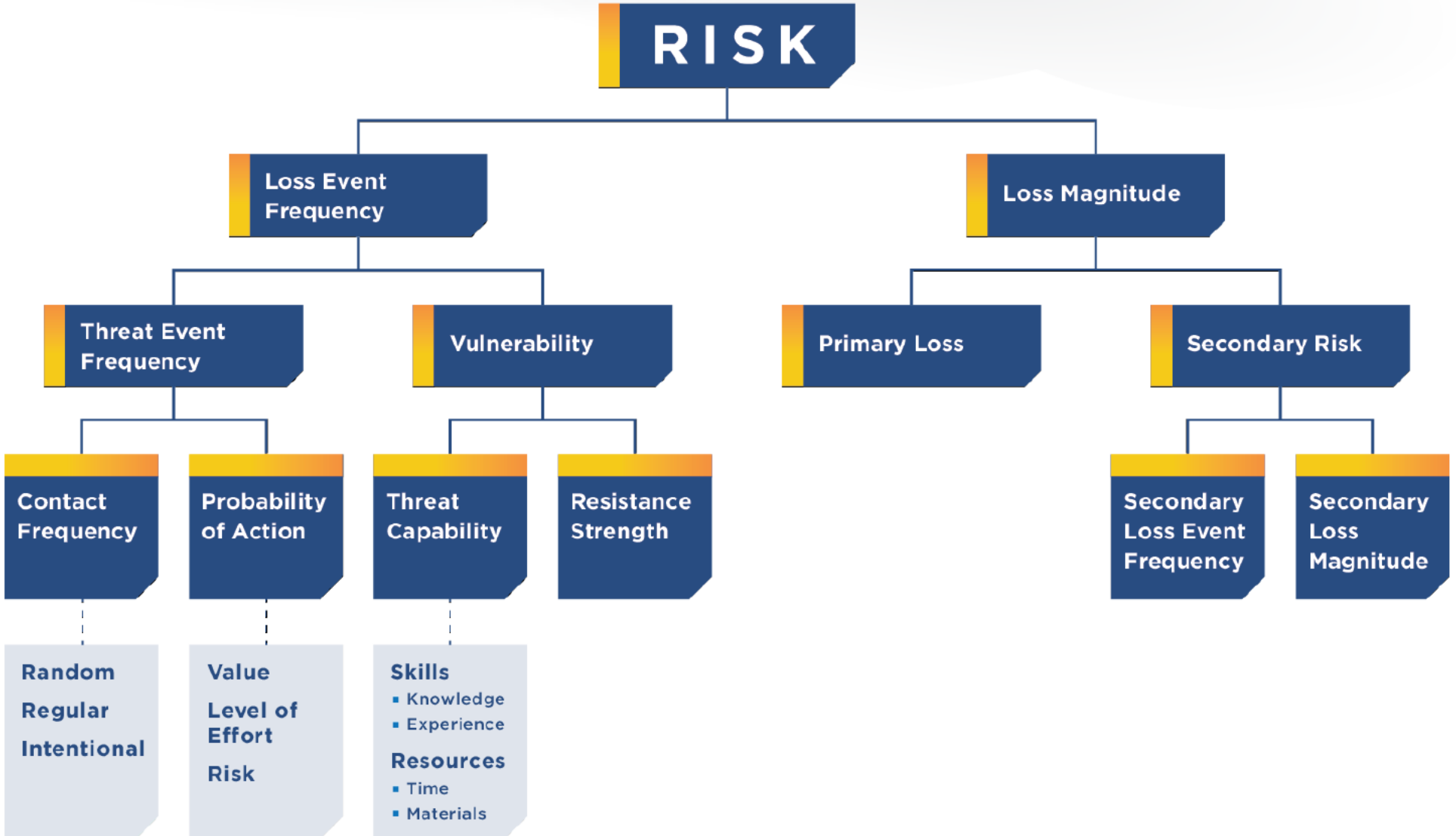


NOW YOU KNOW

RSAConference2020 APJ
A Virtual Learning Experience

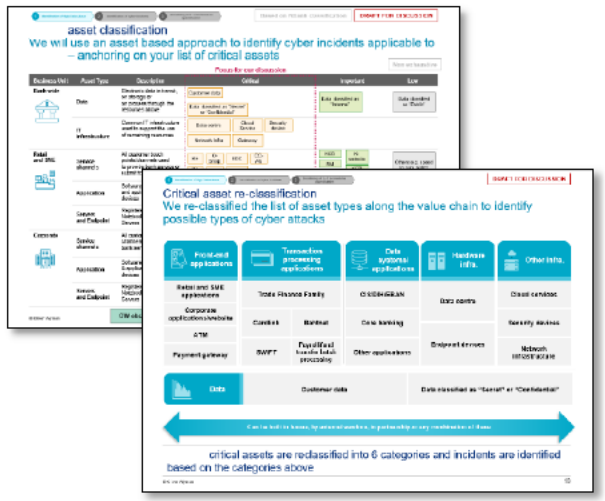
Risk is Shifting with COVID19 Pandemic

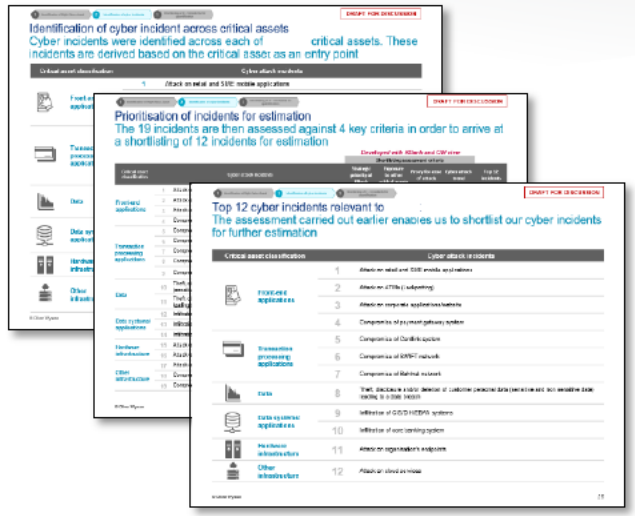
The FAIR Model

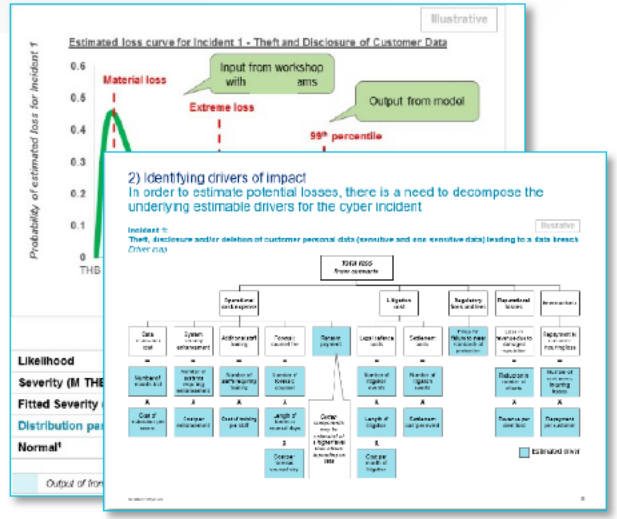


Cyber Risk Assessment for a leading South-East Asian FS player

Non exhaustive







1 Identification of relevant cyber events

- *Based on FS player's high value assets, we derived **new classes of assets** to assess*
- ***Most critical assets** are **used as a proxy** as this would typically result in the **most material losses** if under cyber attack*
- *A **long list of 18 cyber incidents** were identified based on FS player's critical assets*
- *Each of these 18 incidents were assessed against 4 criteria to **shortlist 12 incidents***

2 Scenarios prioritization

- *The 12 incidents shortlisted were then given an **estimated scoring for the frequency and impact** of incident*
- *Based on this scoring, each of the incidents are then mapped against a **3x3 matrix***
- *The **top 3 – 5 incidents** in this matrix will be the basis of our **quantification exercise** in the next step*

3 Impact estimation

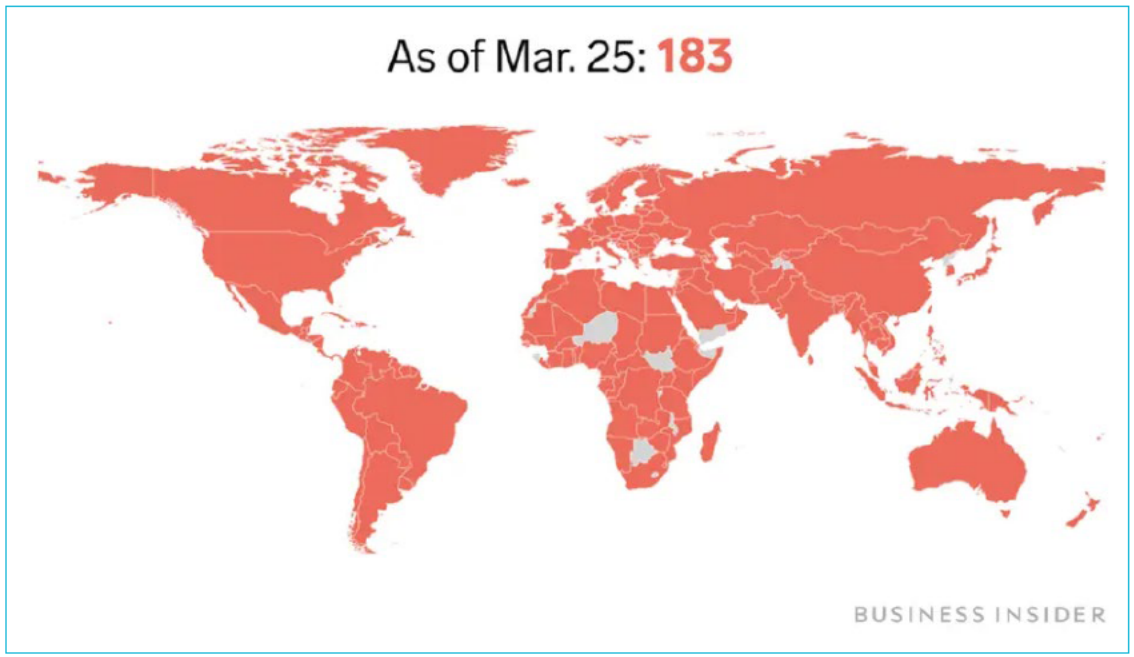
- *Identified workshop participants for each scenario and **conducted scenario workshops** for each Cyber risk event scenario*
- *Used distributions or **point estimates of drivers***
  - *Financial Impact*
  - *Reputational Impact*
  - *Market Participant Impact*
  - *Legal/ liability/ Regulatory Impact*

MARSH

Reality Check – Uncertainty within the Uncertainty

As individuals & organizations around the world fight against the COVID-19 pandemic, other external risks can have an even more disastrous effect to enterprises & critical infrastructure if they occur during a period of crisis; protecting against them remains as important as ever.

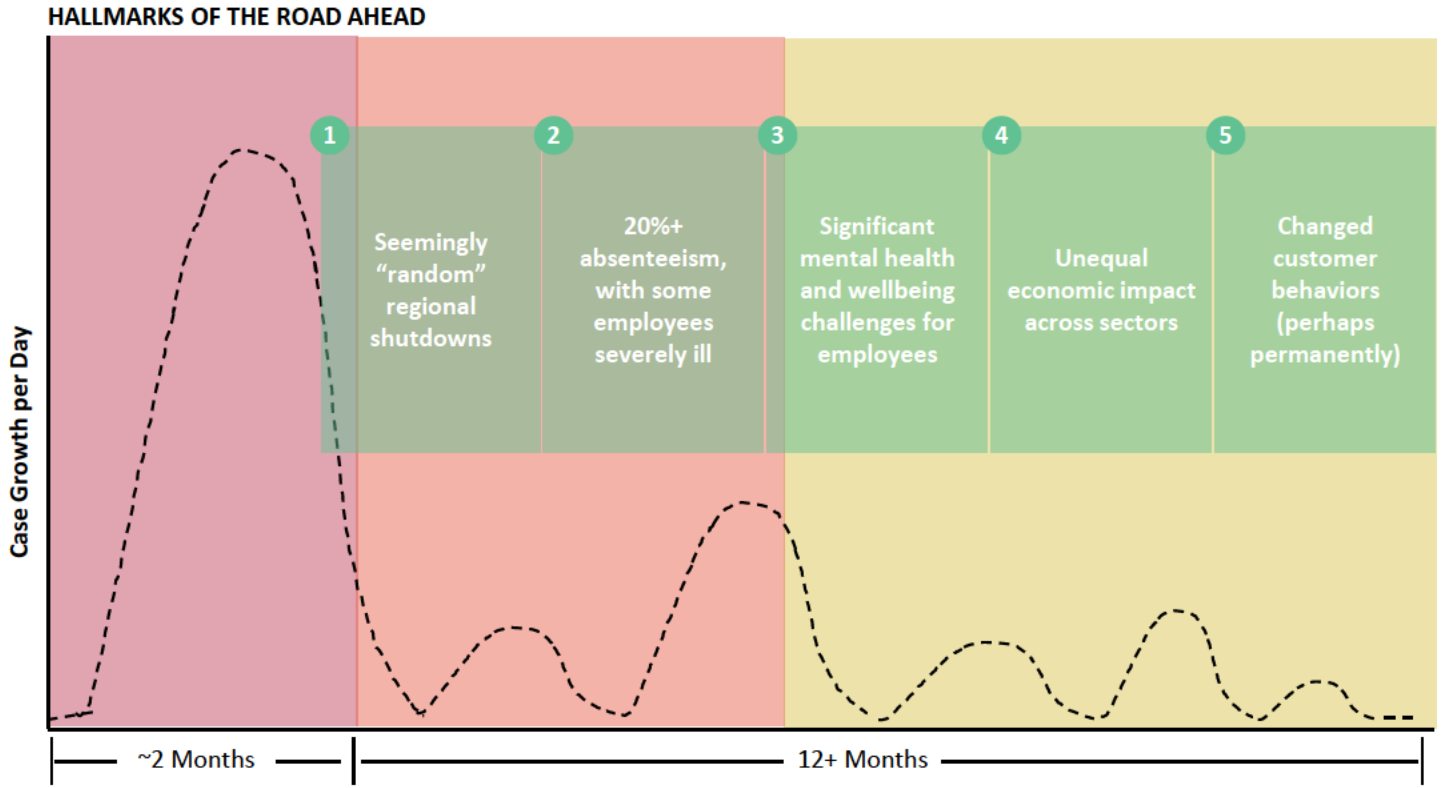
- Social Distancing
- Travel Restrictions
- Crisis Communication
- Changes to Enterprise Budgets
- Public & Cyber Safety Concerns
- Remote Working



First reported in Wuhan, China, on **December 31, 2019**
Declared a global pandemic by the World Heath Organization on **March 11, 2020**

Reality Check – Uncertainty within the Uncertainty

- A pervasive risk of disruption
- Data is required for risk quantification and business impact calculation …



Reality Check –Uncertainty within the Uncertainty

- Shadow IT
- Unsecured Home Networks
- Increased Social Engineering Attacks …

- But, you have already heard about all of those … let me tell you more …

Reality Check – Uncertainty within the Uncertainty

TECH

Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends

PUBLISHED THU, MAR 26 2020•7:58 PM EDT | UPDATED MON, MAR 30 2020•12:17 PM EDT

Arjun Kharpal

SHARE

KEY POINTS

- China mobilized its mass surveillance tools, from drones to CCTV cameras, to monitor quarantined people and track the spread of the coronavirus.
- Other nations like Israel, Singapore and South Korea are also using a combination of location data, video camera footage and credit card information, to track COVID-19 in their countries.
- But privacy experts raised concerns about how governments were using the data, how it was being stored and the potential for authorities to maintain heightened levels of surveillance — even after the coronavirus pandemic is over.

Reality Check – Uncertainly within the Uncertainty

- New Privacy Laws
- Data Breach Notifications
- PII Definitions & Clarifications
- Third-Party Breach Liabilities
- Cross-Border Limitations

Reflecting on APAC Data Protection and Cyber-security Highlights for 2019 (and what lies ahead!)

By Anna Gamvros (HK) and Libby Ryan (HK) on January 20, 2020
Posted in General

2019 saw continued growth and change in data protection and cyber-security across the Asia-Pacific. Following the implementation of the GDPR in May, 2018, many jurisdictions moved to review and strengthen existing data privacy and cyber-security laws. In addition, 2019 saw regulators publishing findings in respect of some of the largest data incidents of 2018. We have set out below the key highlights of the year and what to look out for in 2020.

January Singapore

Singapore's Personal Data Protection Commission ("**PDPC**") imposed the highest fines to date in respect of a cyber-attack on SingHealth's patient

It is Again all about Risks ….

Threat	Scenario	Scenario Details & Impact
Ransomware / Malware	A malware infects multiple segments of the CCTV security network; intending to encrypt system files and data	The company updates one of its servers with a compromised update (ransomware) The ransomware spreads into the company's network, using some unpatched vulnerabilities The ransomware is executed on company's systems and devices and steal stored credentials The ransomware executes a mechanism of elevation of privileges, using bad segregation of highly privileged accounts The ransomware spreads into other part of the company's network by the same mechanism The infected systems and devices are encrypted and cannot be used anymore A ransom is required while all the systems and devices are down

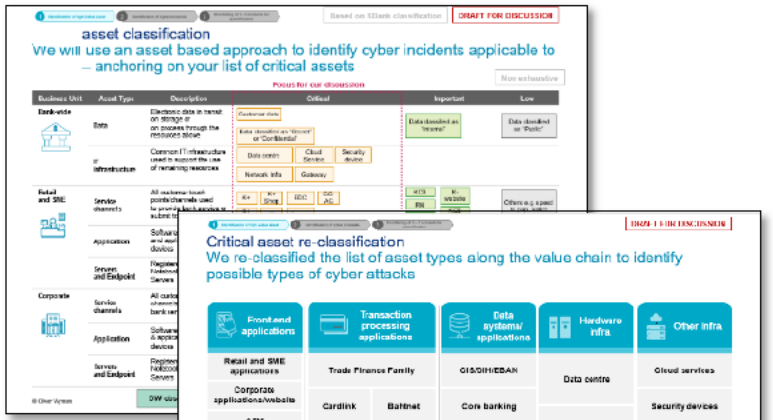

WATCHING YOU

RSAConference2020 APJ

A Virtual Learning Experience

The Perimeter Is Dead: Security Without Boundaries

Cyber Risk Assessment for a leading South-East Asian FS player in a COVID19 Era



1 Identification of relevant cyber events

2 Scenarios prioritization

- **Data Loss**, due to an unauthorized usage of BYOD with work from policies
- **Ransomware Attack**, due to an unauthorized physical access to the corporate office
- **Business Interruption**, due to a vulnerable unpatched workstation (Patch failure, due to unavailability of access to corporate network)

MARSH

Cyber Risk Assessment for a leading South-East Asian FS player in a COVID19 Era

Business Interruption
- Loss of Gross Profits
- Overtime
- Marketing & Promotional Expenses
- Less: Fixed Cost Savings

Total Business Interruption Cost

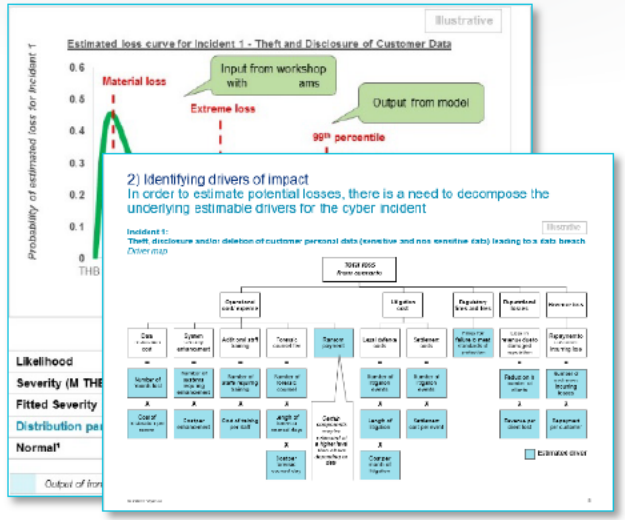
First Party Costs
- Litigation Costs
- Forensics Investigation
- Ransomware Costs
- Call Centre Costs
- Public Relations
- Claims Preparation Costs

Total First Party Related Cost

Data Leak Cost
- Notification Cost
- Credit Monitoring
- Regulatory Actions - Civil / Administrative Sanctions

Total Data Leak Cost

Total Cyber Risk Exposure



3 Impact estimation

- *Identified workshop participants for each scenario and **conducted scenario workshops** for each Cyber risk event scenario*
- *Used distributions or **point estimates of drivers***
  - *Financial Impact*
  - *Reputational Impact*
  - *Market Participant Impact*
  - *Legal/ liability/ Regulatory Impact*

Focus on the Data and the Human

- **Data Loss**, due to an unauthorized usage of BYOD with work from policies
  - ✓ **Newsletters do not work !**
- **Ransomware Attack**, due to an unauthorized physical access to the corporate office
  - ✓ **Deserted offices need additional controls !**
- **Business Interruption**, due to a vulnerable unpatched workstation
  - ✓ **Implement Hardware Based Security (Data Diode ?)**

RSAConference2020 APJ

A Virtual Learning Experience

Data-Driven Security with Zero Trust is the Future

A New Approach

- **Adopt a data-centric approach** – It is all about data
- **Improve authentication** – Get the MFA working
- **Use advanced tools** - Get secure access to internal applications ensuring usability
- **Promote education and training** – It never changes, but be reachable for your employees

Apply What You Have Learned Today

- Next week you should:
  - Identify your new emerging cyber risks
- In the first three months following this presentation you should:
  - Ensure a non-perimeter based security approach
  - Start thinking about zero trust
- Within six months you should:
  - Have a cyber security strategy around data security