

Data Leakages from the Cloud - Forgotten Child in Cloud Security

Wong Onn Chee

CEO, Rajah & Tann Cybersecurity (onnchee@rtcyber.com)

CTO, Resolvo Systems (onnchee@resolvo.com)

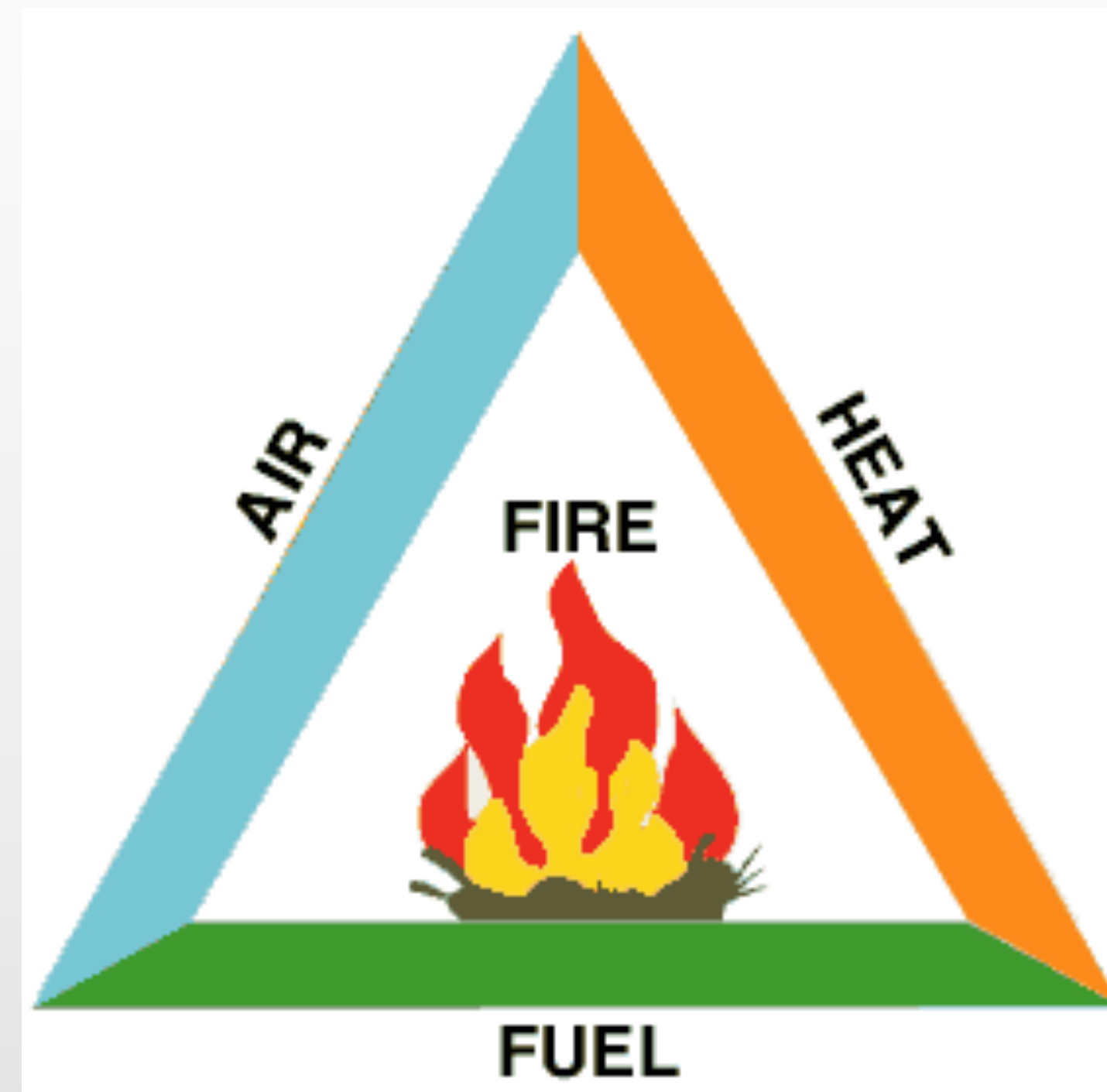
Co-Chair, CSA Government Affairs Advisory Council

CSA cloud
security
alliance®

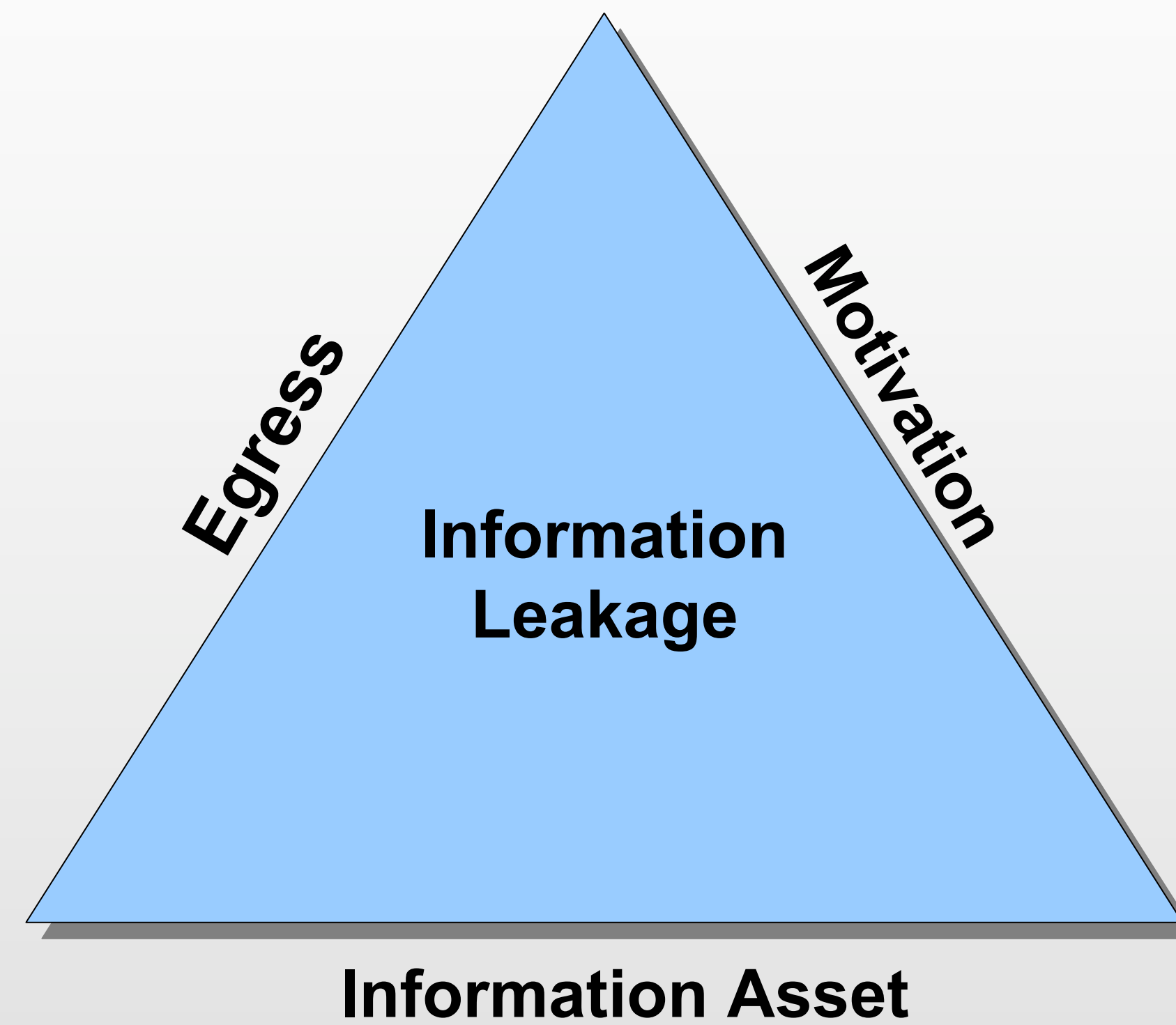
Agenda

- Information Leakage Triangle
- (In)famous cases of data leakages from cloud
- DEFICT Framework
- Application of DEFICT Framework to actual cases

Fire Triangle



Information Leakage Triangle

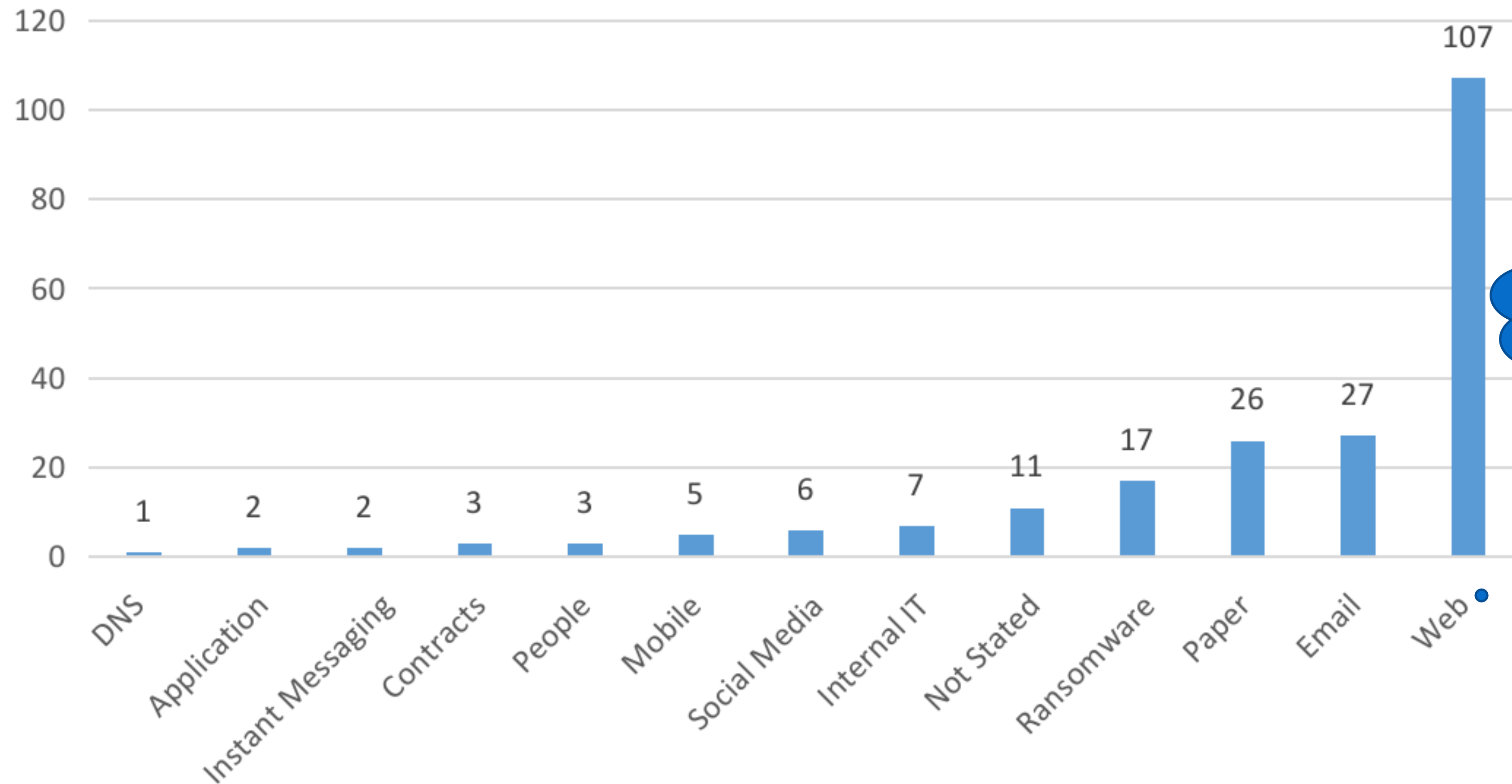


PDPC Enforcement Decisions to date

- Excluding non-monetary directions or non-breaches, PDPC has imposed S\$3,328,400.00 in financial penalties across 217 cases as at 17 April 2023, since the 1st published decision on 21 April 2016.

PDPC Enforcement Decisions to date

Enforced Cases by Channel of Breach



Includes cloud-hosted web servers

An egregious example of cloud leakage

Bloomberg US Edition

● Live Now Markets Economics Industries **Technology** Politics Wealth Pursuits Opinion Businessweek Equality Gree

Technology
Cybersecurity

Hackers Claim Theft of Police Info in China's Largest Data Leak

- Unknown cyberattackers claim to have info on a billion Chinese
- The claim triggered speculation online and in security circles

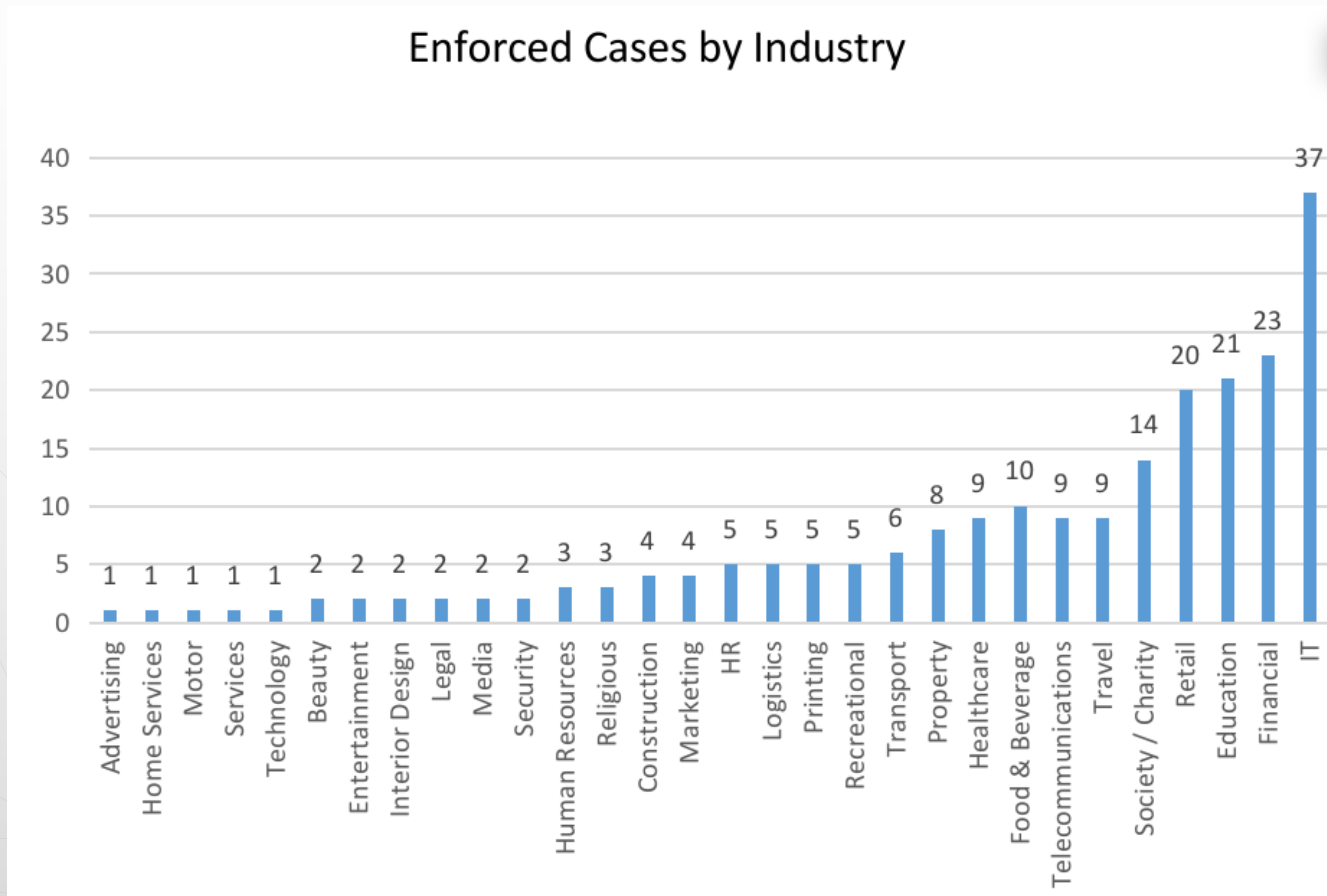


WATCH: Hackers claimed to have stolen data on as many as a billion Chinese residents after breaching a police database. Edwin Chan reports. *Source: Bloomberg*

By Sarah Zheng
July 4, 2022 at 1:27 PM GMT+8

Source:
<https://www.bloomberg.com/news/articles/2022-07-04/hackers-claim-theft-of-police-info-in-china-s-largest-data-leak?leadSource=verify%20wall>

PDPC Enforcement Decisions to date

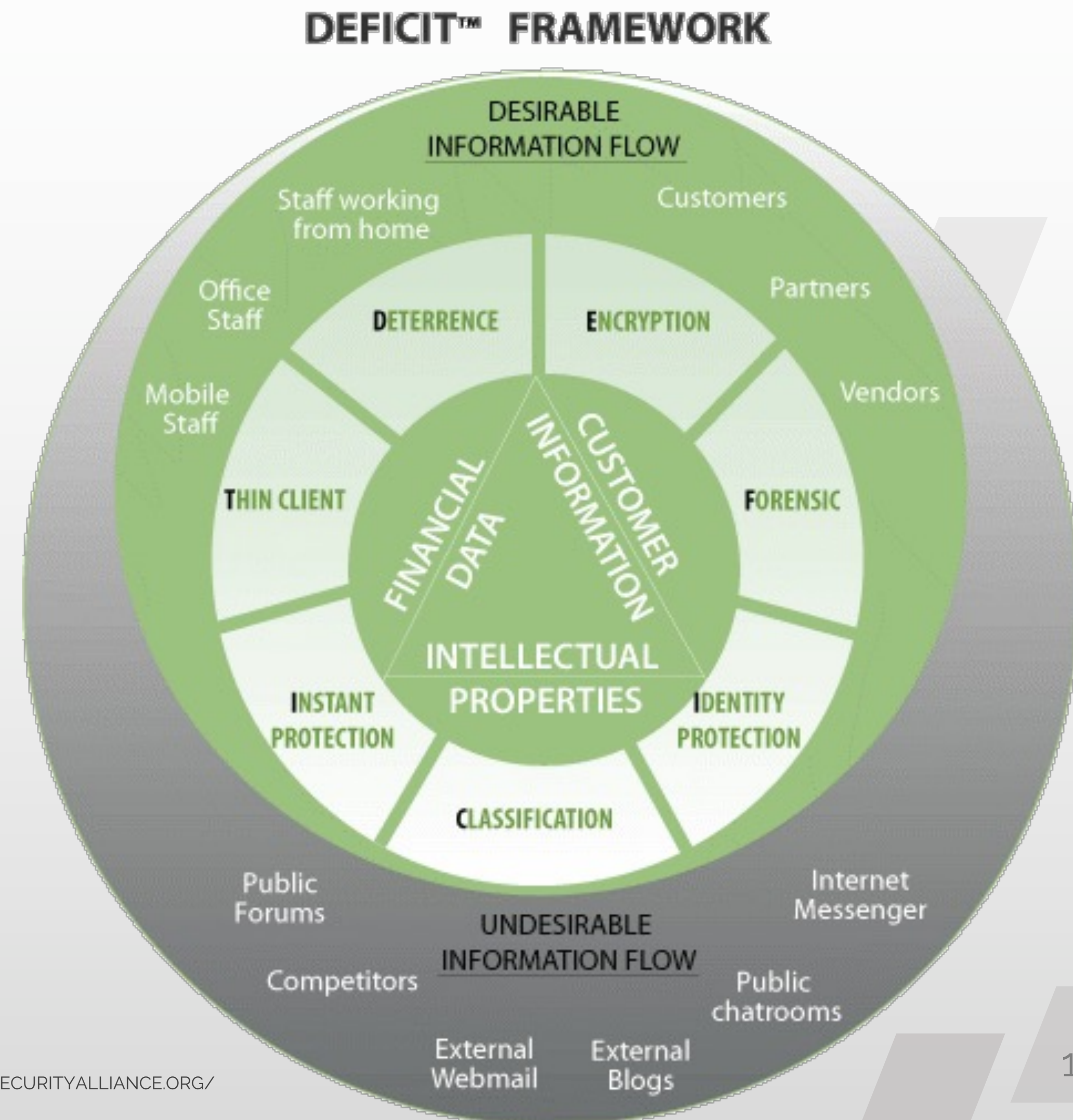


DEFICIT Framework

1. A practical data protection framework we used to advise clients.
2. Can be applied to cloud or on-prem environment.

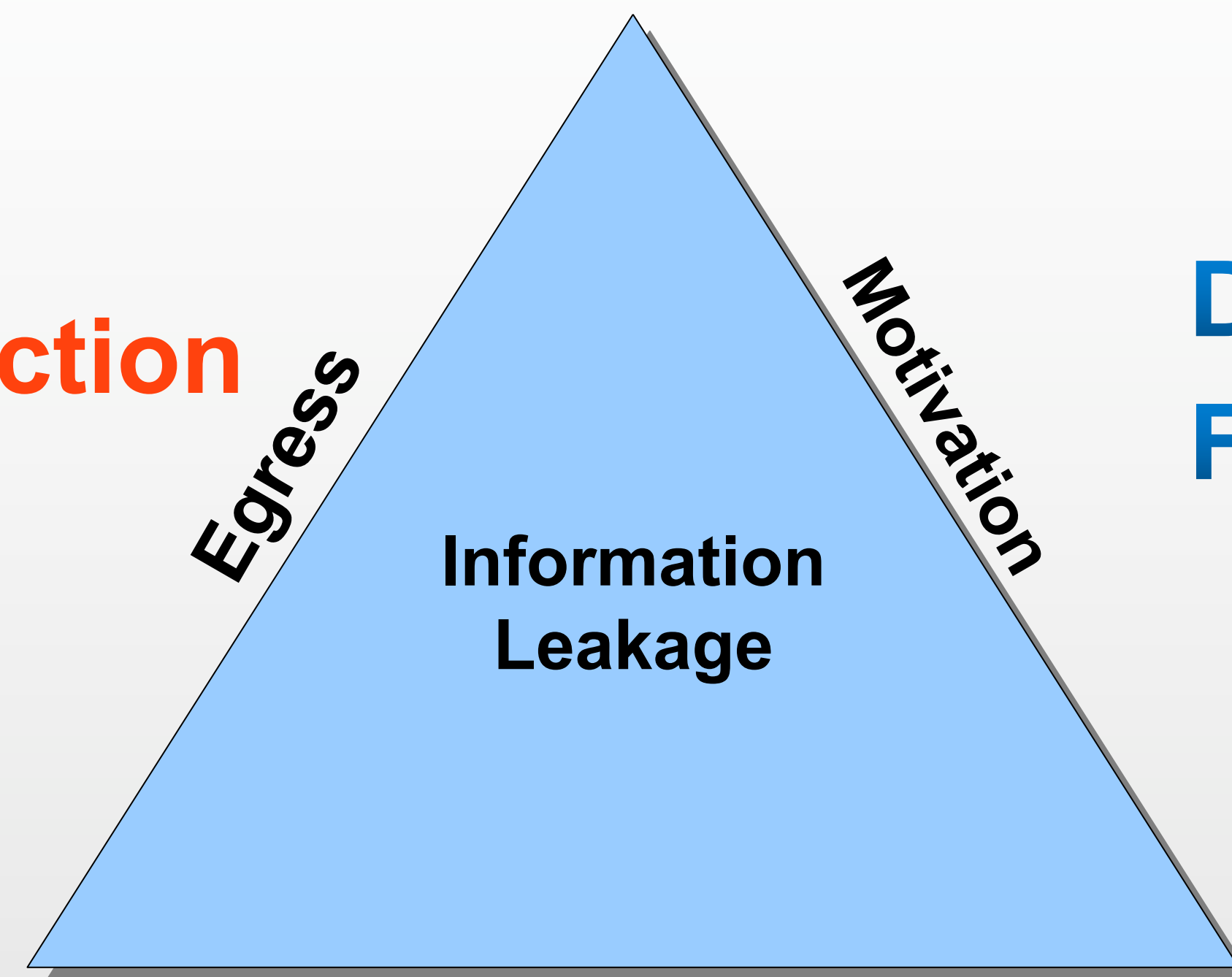
DEFICIT Framework

- **D** eterrence
- **E** nryption
- **F** orensics
- **I** nstant protection
- **C** lassification
- **I** dentity Protection
- **T** hin Clients



DEFICIT Framework + IL Triangle

Encryption
Forensics
Intity Protection
Classification
Intant
Protection
Thin Clients

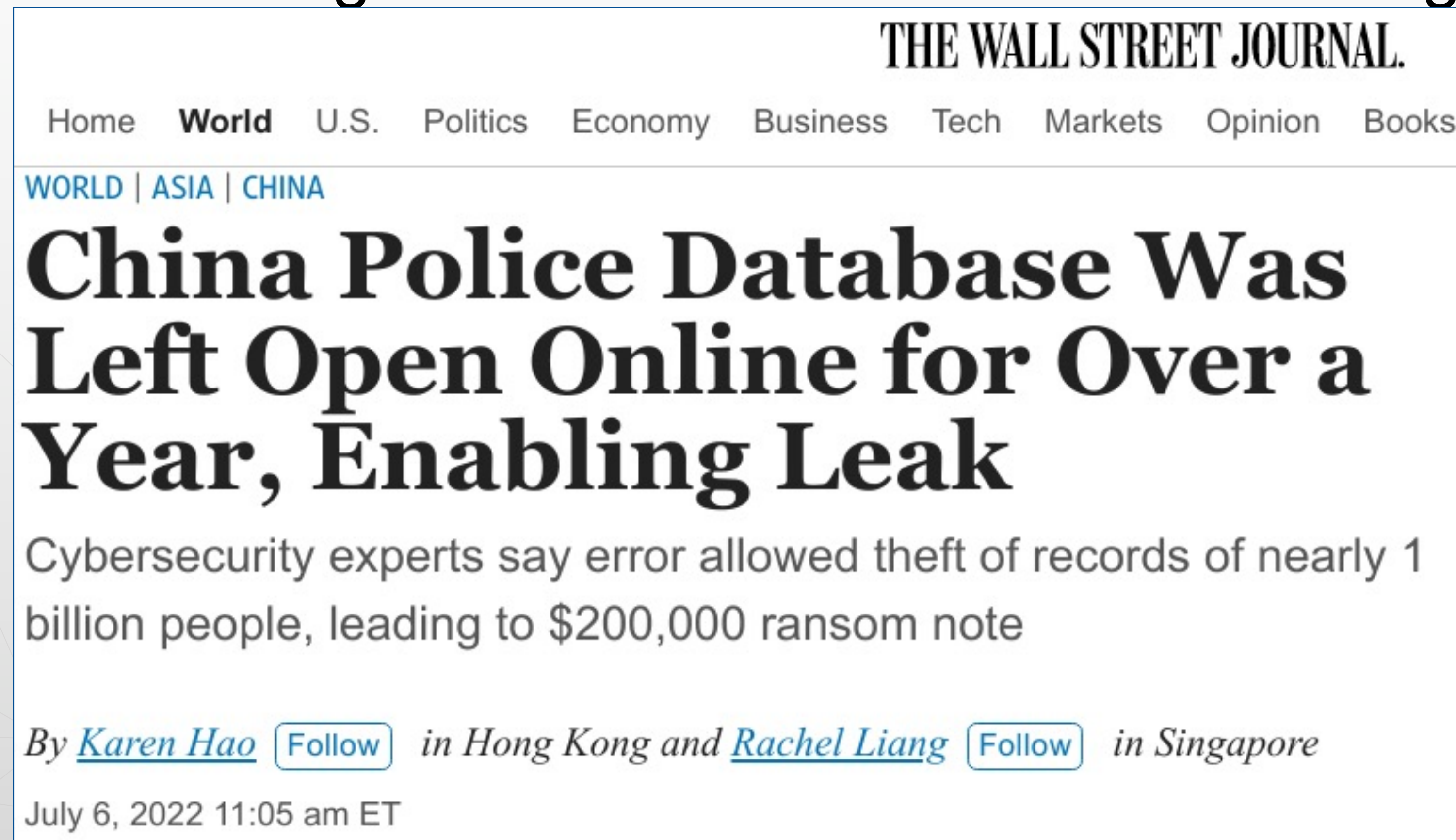


Deterrence
Forensics

Information Asset
Encryption
Forensics
Classification

Case Study 1: Shanghai Police Department

Researchers found that the database itself was secure, but that a management dashboard was publicly accessible from the open internet, allowing anyone with basic technical skills to grab the information without needing a password.



THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Books

WORLD | ASIA | CHINA

China Police Database Was Left Open Online for Over a Year, Enabling Leak

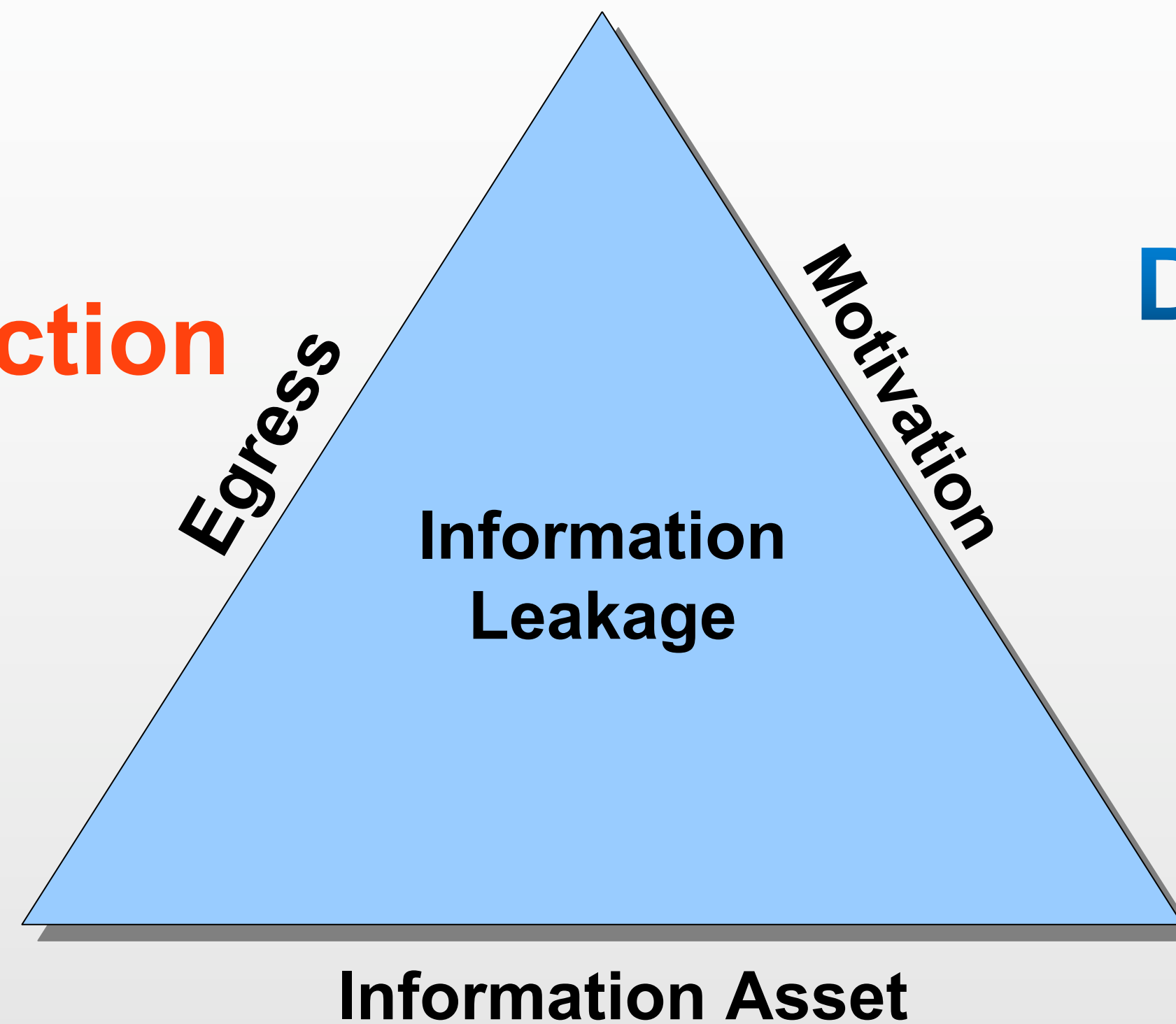
Cybersecurity experts say error allowed theft of records of nearly 1 billion people, leading to \$200,000 ransom note

By [Karen Hao](#) [Follow](#) in Hong Kong and [Rachel Liang](#) [Follow](#) in Singapore

July 6, 2022 11:05 am ET

Case Study 1: Shanghai Police Department

Identity Protection
Classification
Instant Protection



Deterrence

Case Study 2: Accenture

The exposed Amazon S3 storage services contained hundreds of GB of sensitive data, including secret API data, authentication credentials, certificates, decryption keys, customer information, and more.

Accenture data leak: 'Keys to the kingdom' left exposed via multiple unsecured cloud servers

BY INDIA ASHOK ON 10/11/17 AT 7:24 AM

```
mirror_mod = modifier_ob.modifiers.new("mirror_mod")
mirror_mod.mirror_object = mirror_ob

operation -- "MIRROR_X":
  mirror_mod.use_x = True
  mirror_mod.use_y = False
  mirror_mod.use_z = False
operation -- "MIRROR_Y":
  mirror_mod.use_x = false
  mirror_mod.use_y = True
  mirror_mod.use_z = False
operation -- "MIRROR_Z":
  mirror_mod.use_x = false
  mirror_mod.use_y = false
  mirror_mod.use_z = True

# Selection at the end -add back the deselection
mirror_ob.select = 1
mirror_ob.select = 1
key.context.scene.objects.active = modifier_ob
key.selected = str(modifier_ob) + modifier_ob
mirror_ob.select = 0
key.context.selected_objects[0]
key.objects[one.name].select = 1

print("please select exactly two objects,")
```

Case Study 2: Accenture

Identity Protection

Instant Protection

Egress

Motivation

Deterrence

Information Leakage

Information Asset Encryption

Classification

Case Study 2: Accenture

This issue was not new. Similar cases were reported years before.

Amazon Simple Storage Buckets Leak Owner's Data

By: [Bogdan Botezatu](#) | comment : 0 | March 29, 2013 | Posted in: [Industry News](#)

Almost 2,000 storage buckets from cloud provider Amazon are inadvertently exposing confidential user data due to improper configuration by the customer, according to a study by Metasploit vendor Rapid7.



Buckets are logical storage containers that companies use for purposes from mirroring downloads to storing office documents or local backups. They can be set as either public or private, and access to the files is granted as such. If they are set as public, the bucket's contents can be listed and accessed by anyone who knows the URL of the bucket. The URL can easily be deduced as it follows a predefined format (such as [http://s3.amazonaws.com/\[bucket_name\]/](http://s3.amazonaws.com/[bucket_name]/) or [http://\[bucket_name\].s3.amazonaws.com/](http://[bucket_name].s3.amazonaws.com/)), it's easy to predict the bucket's URL by running names in a dictionary, for instance.

Proposed playbook to data leakages from cloud

1. Remove leaking file immediately OR take the affected website offline and isolate immediately.
2. Show last good copy or show a user-friendly maintenance page.
3. Clone the offline affected server and perform forensics analysis on the cloned copy.
4. Analyse the network and web server access logs to identify where the data was leaked to.
5. Monitor search engines, public forums, dark web, social media and P2P file sharing networks for any public sharing of leaked

Proposed playbook to data leakages from cloud

6. Assess the privacy impact of the leakage and inform the persons affected by the leakage.
7. Report to PDPC or sector regulators, such as MAS.
8. Submit forensics evidence to the police if it is due to malicious attacks, including the identified source of attacks.
9. Identify the last good copy backup of the cloud site content and restore the last good backup onto new web instances and/or database instances. **DO NOT** go live with the restored site yet.
10. Remove any identified backdoor or vulnerability from the restored copy and apply patches if new ones are available.

Proposed responses to data leakages from cloud

11. Harden the web application server and its host OS.
12. Perform vulnerability assessment and penetration testing of the restored cloud site.
13. Ensure any new settings on the network defenses are properly configured.
14. Go live with restored cloud site.
15. Implement tighter content upload procedures, e.g. 4-eyes principle for all content upload.
16. Implement egress monitoring on all outbound responses after cloud site is restored.

THE END

Data Leakages from the Cloud - Forgotten Child in Cloud Security

Thank You for Your Attention

CSA cloud security alliance®