

*ASCO - IT Security for
Intermediaries*
Knowledge Sharing

November 2018



Agenda

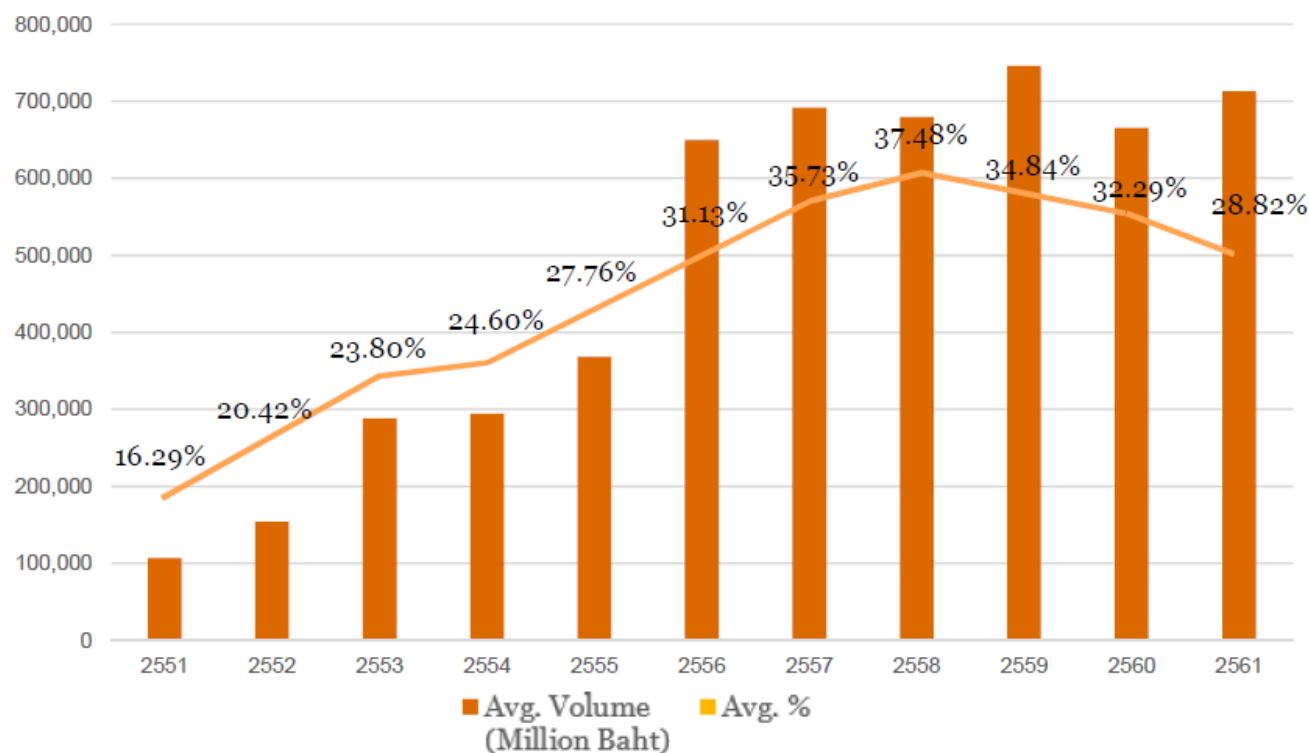
Why IT Security?

Cyber Resilience

Common Industry Observations

Why IT Security?

Contribution of Electronic Trading System



https://www.set.or.th/th/market/market_statistics.html

Why IT Security?

Penny Stock Pump-and-Dump Scheme

MARKETS | FINANCIAL REGULATION

Penny-Stock Promoter Pleads Guilty to Manipulating Companies

Gregg R. Mulholland could face up to 20 years in prison in 'pump and dump' scheme

By *Christopher M. Matthews*

May 9, 2016 4:05 p.m. ET

A penny-stock promoter pleaded guilty Monday to conspiring to manipulate stocks laundering more than \$250 million in profits, in what prosecutors have described as the largest-ever "pump and dump" schemes.

<https://www.wsj.com/articles/penny-stock-promoter-pleads-guilty-to-manipulating-companies-1462824337>



<https://in.reuters.com/article/cyber-brokerages-hongkong-idINKBN15U0BA>

ASCO - IT Security for Intermediaries

Hired hackers key to JP Morgan, Fidelity breaches

By *REUTERS*

New York/San Francisco, 16 Nov 2015



The hackers stole data on 83 million customers from JP Morgan alone.

When US prosecutors this week charged two Israelis and an American fugitive with raking in hundreds of millions of dollars in one of the largest and most complex cases of cyber fraud ever exposed, they also provided an unusual look into the burgeoning industry of criminal hackers for hire.

The trio, who are accused of orchestrating massive computer breaches at JPMorgan Chase and other financial firms, as well as a series of other major offences, did little if any hacking themselves, indicate the federal indictments and a previous civil case

brought by the US Securities and Exchange Commission.

<https://www.itweb.co.za/content/nkLgB1Meg26v59N4>

Crooked 'pump and dump' trades double to HK\$53m in Hong Kong

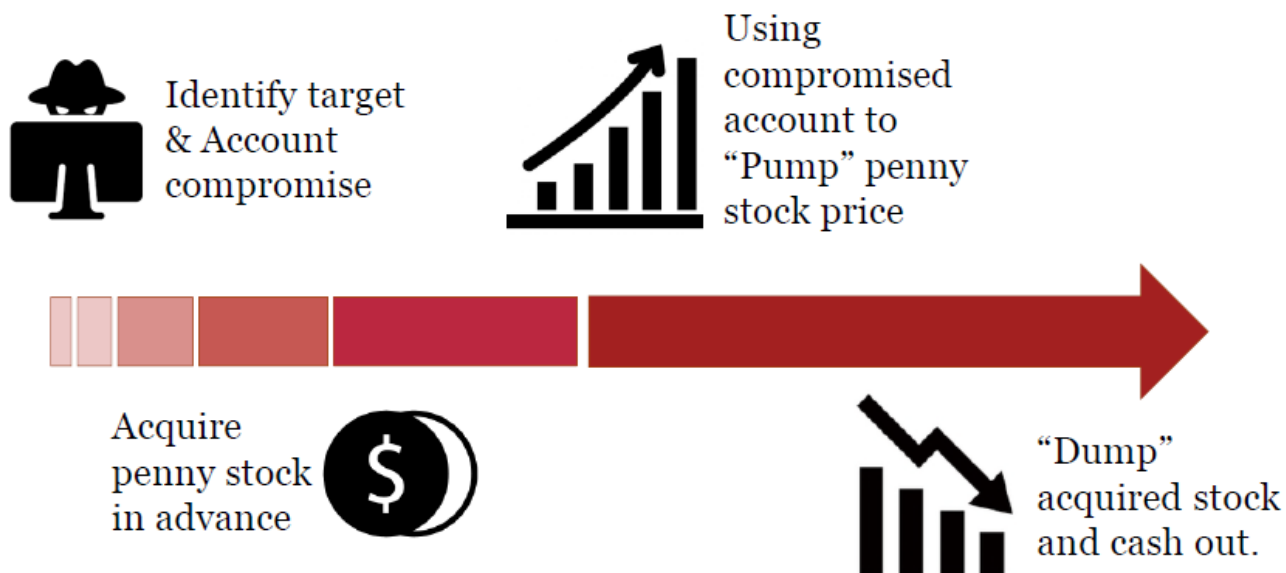
The discovery has prompted officials to warn the public to guard against hackers when using electronic devices.

<https://www.scmp.com/news/hong-kong/law-crime/article/1982323/crooked-pump-and-dump-trades-double-hk53m-hong-kong>

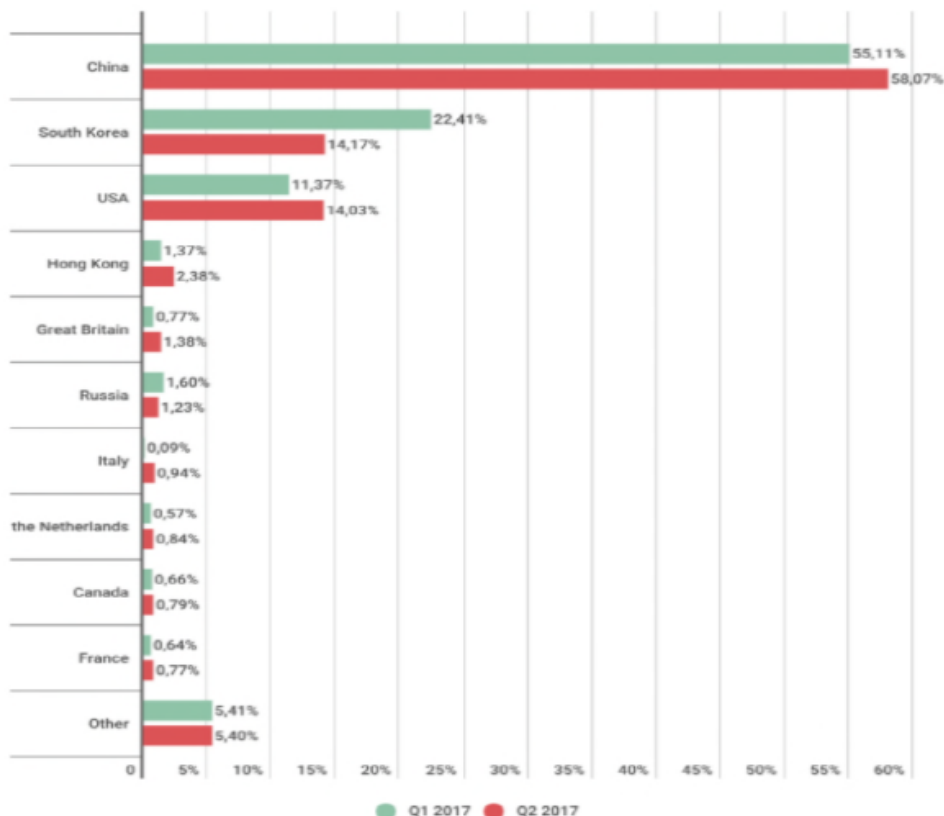
November 2018

Pump-and-Dump

How was money stolen from the account?



DDoS attacks



Hong Kong brokers are being repeatedly targeted by hackers

Five Taiwan brokerages report DDoS cyber attack threats, regulator says

Lloyds Banking Group Reportedly Hit by DDoS Attack

DDoS Attacks Slam Finnish Bank

Ukraine Blackout Redux: Hacking Confirmed

PYONGYANG LAUNCHES ATTACK AGAINST BITCOIN

DDoS attacks were registered in 86 countries in Q2, where the largest number of the attacks were aimed at China (58.07% of all of the attacks), which is 3 p.p. higher compared to the previous quarter. South Korea went down from 22.41% to 14.17% and retained second place nonetheless, while the USA rose from 11.37% up to 14.03%, almost catching up with South Korea.

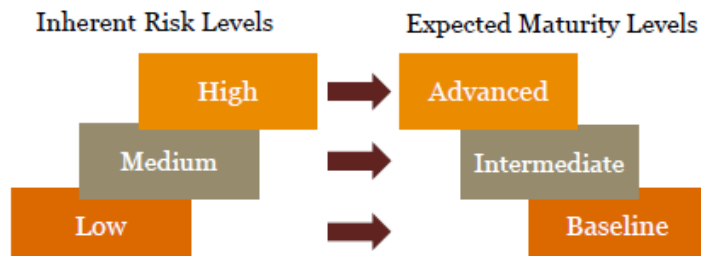
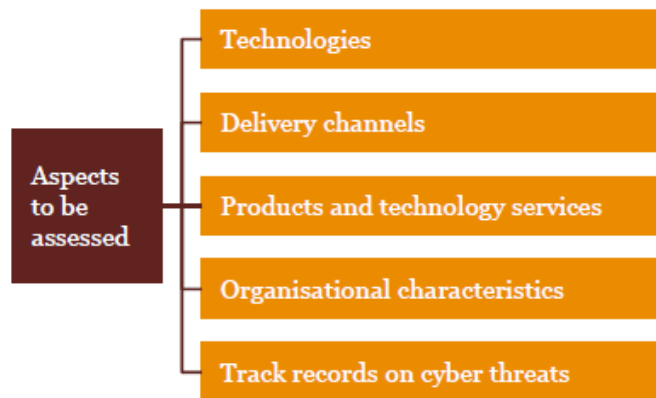
Source: Kaspersky (<https://securelist.com/ddos-attacks-in-q2-2017/79241/>)

Cyber Resilience

It's all about risks

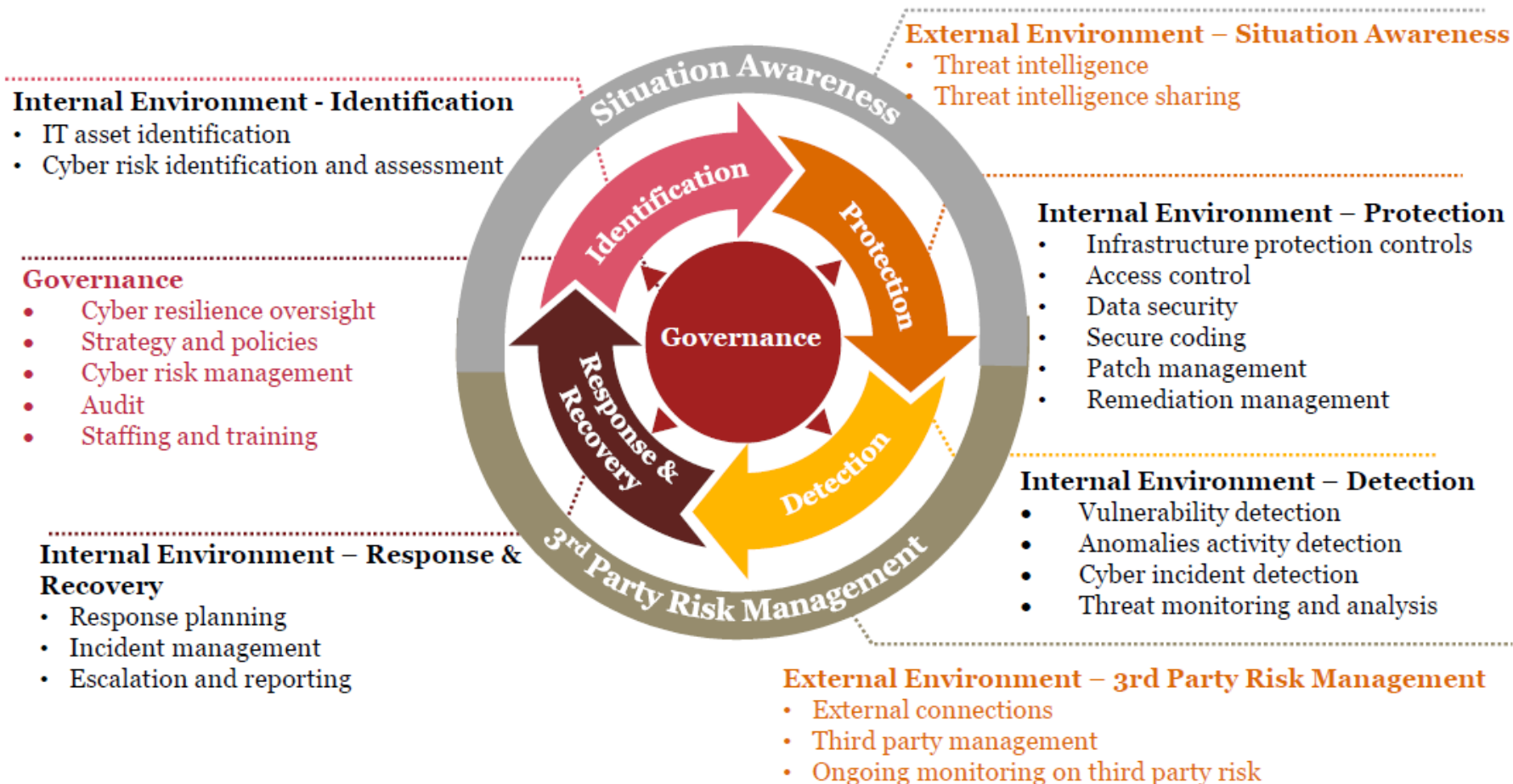
1 Inherent risk assessment

2 Control Maturity



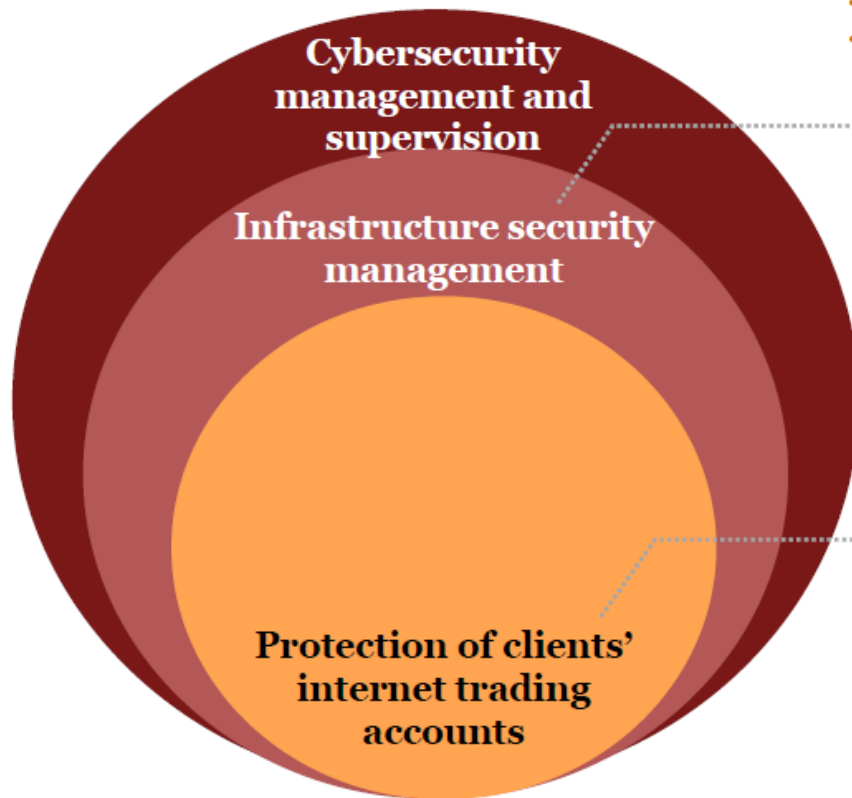
Cyber Resilience

The Cyber Resilience Framework



Cyber Resilience

Area of Focus



- Roles and responsibilities of cybersecurity management
- Cybersecurity incident reporting
- Cybersecurity awareness training for internal system users
- Cybersecurity alert and reminder to clients

- Deploy a secure network infrastructure
- User access management
- Security controls over remote connection
- Patch management
- End-point protection
- Unauthorized installation of hardware and software
- Physical security
- System and data backup
- Contingency planning for cybersecurity scenarios
- Third-party service providers

- Authentication
- Implement monitoring and surveillance mechanisms
- Prompt notification to clients
- Data encryption
- Protection of client login passwords
- Stringent password policies and session timeout controls

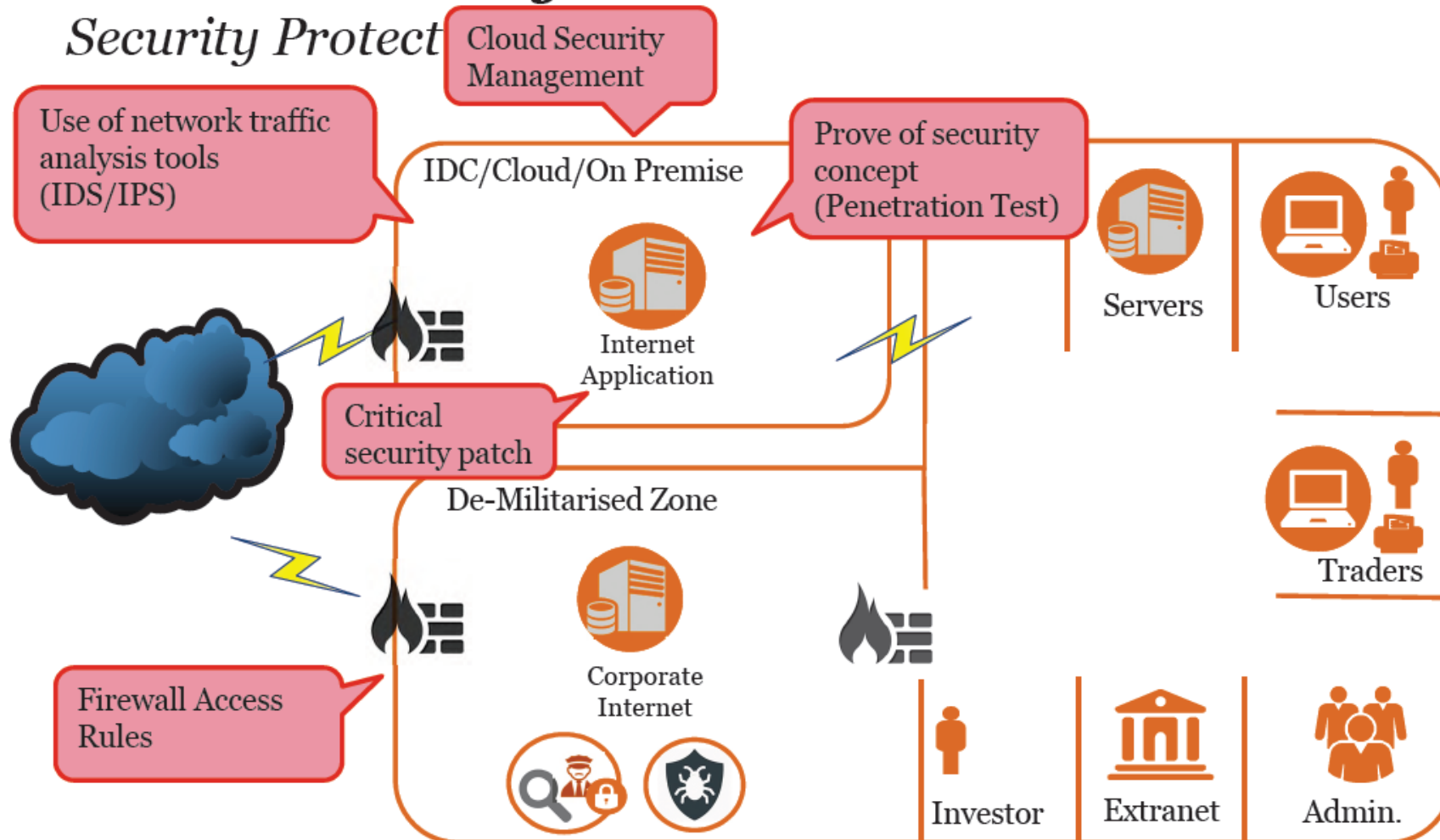
Common Industry Observations

IT Governance



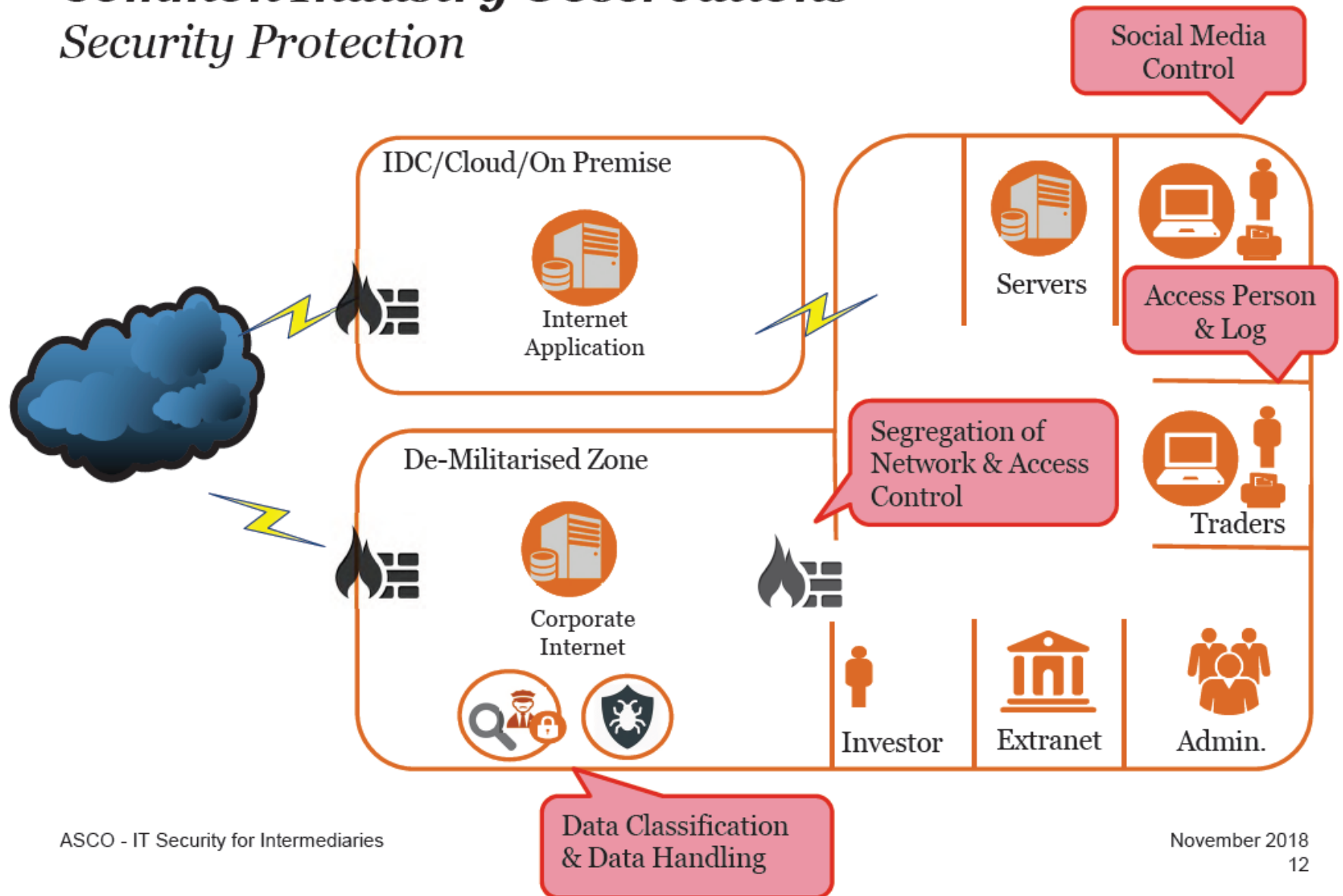
Common Industry Observations

Security Protect



Common Industry Observations

Security Protection



Q & A