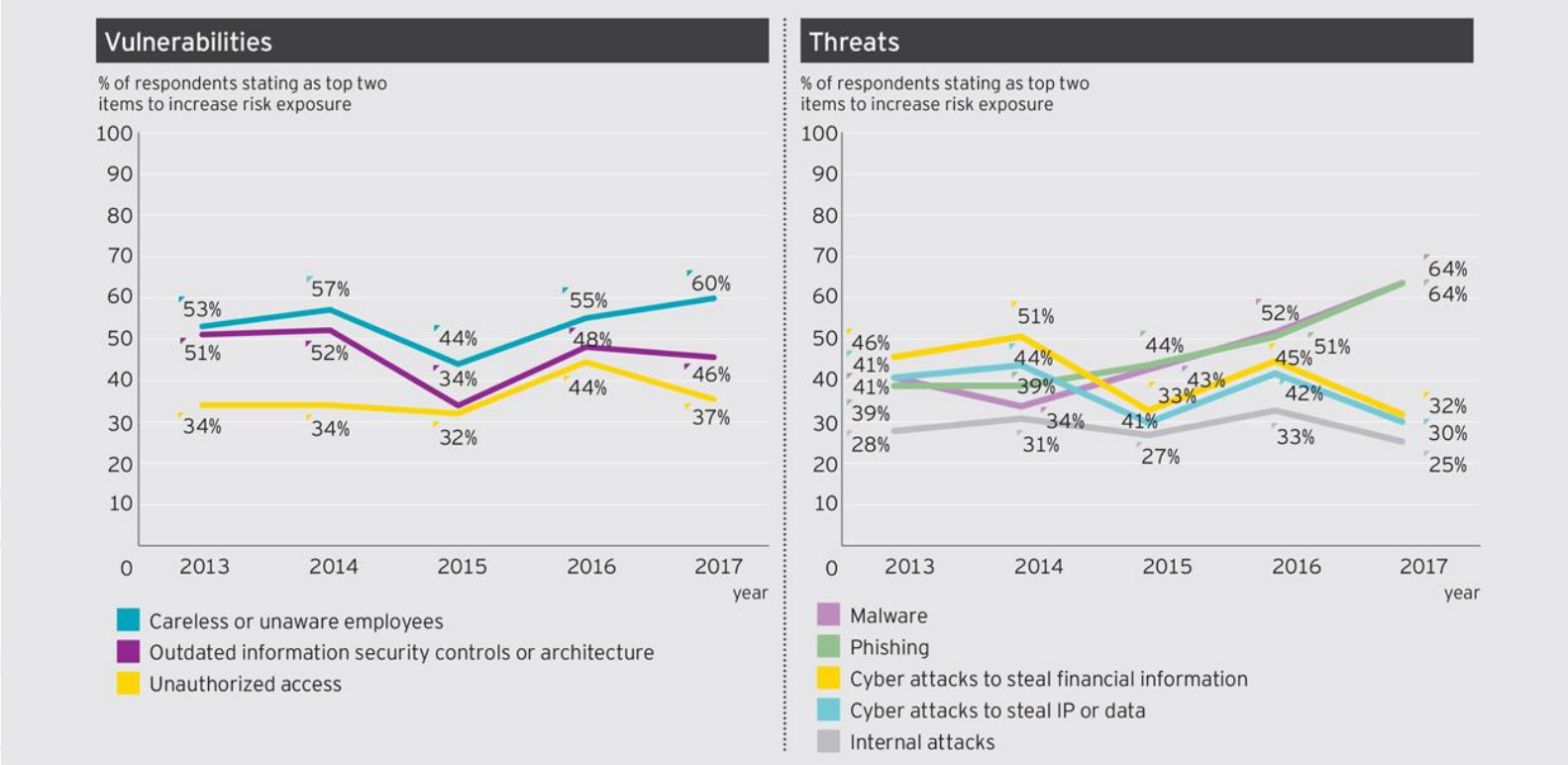
Safeguarding your Organization's Network Perimeter – From Outside and Inside

Brian Chong

Agenda

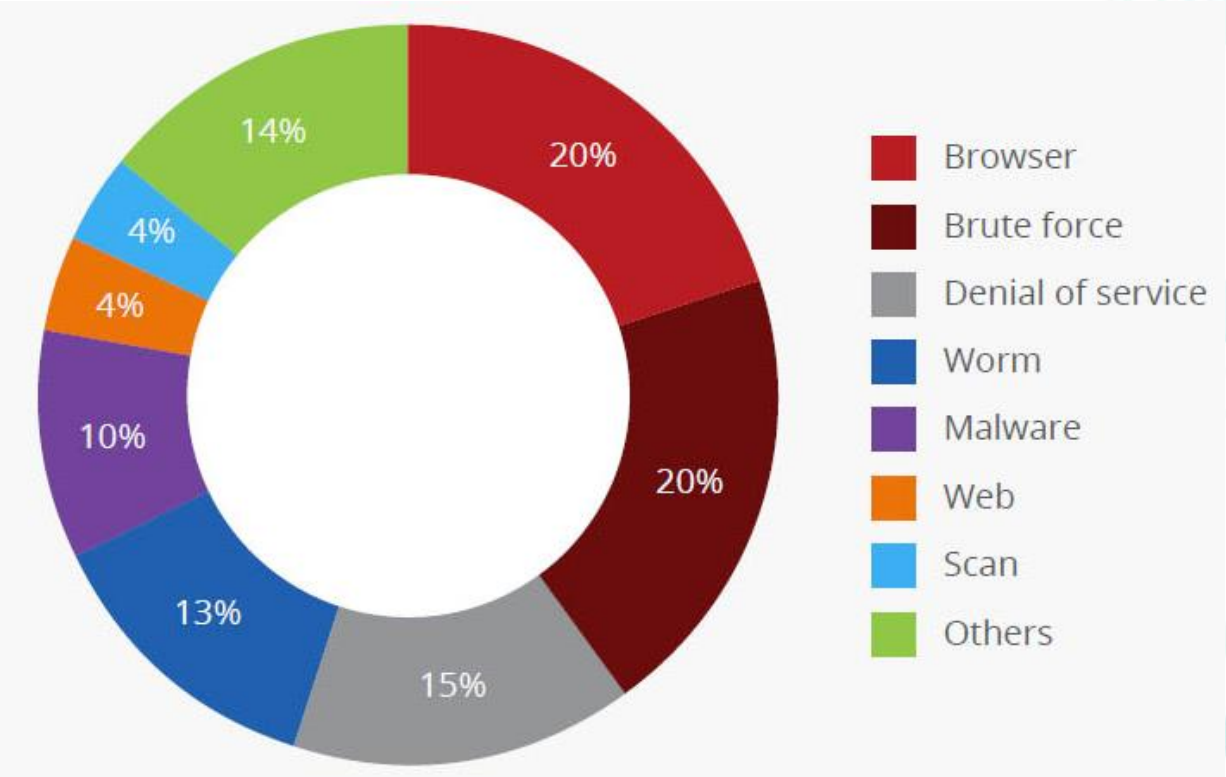

01
Protection on the network
02
Protection at the endpoint
03
Operations consideration
04
Challenge faced by SME

Trends of Threats and Vulnerabilities



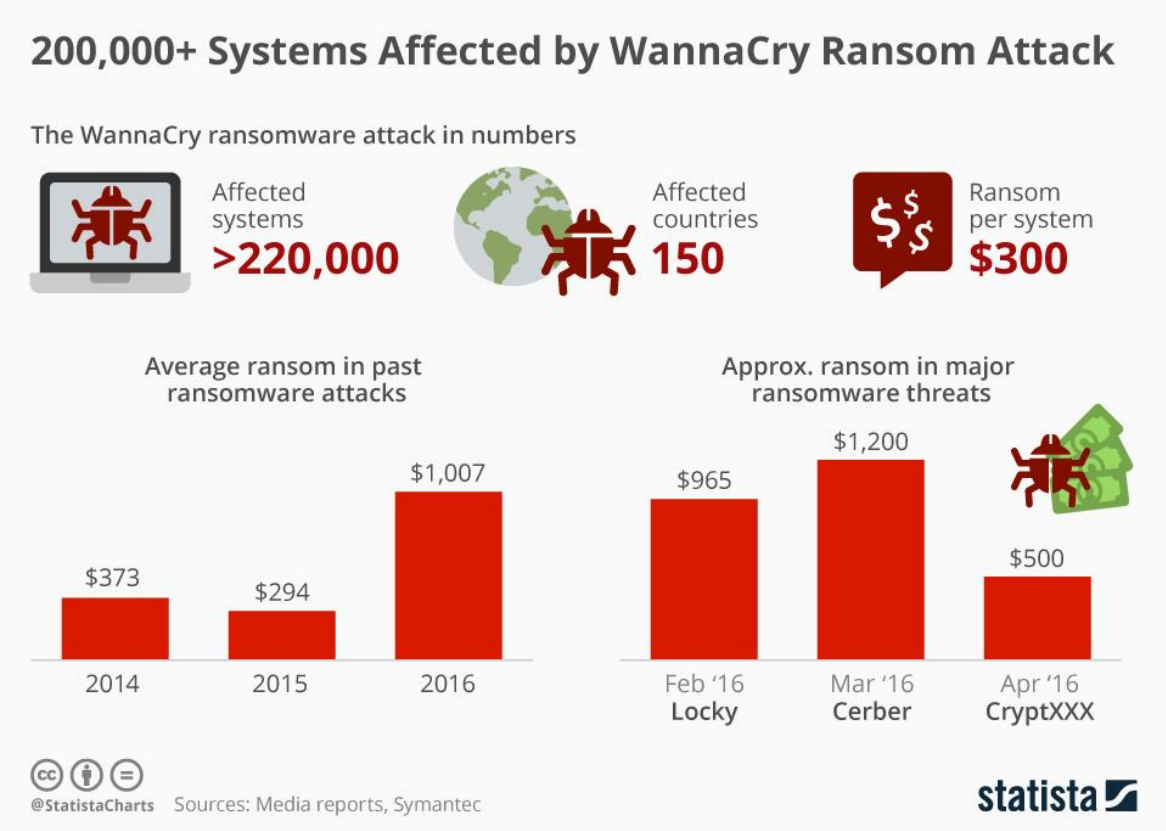
Source: EY

Top 8 Types of Network Attacks



Source: McAfee (2017)

Do you still remember WannaCry?



Other Incidents in HK / World

Nov 2017

港旅行社首遭黑客入侵　業界嚴防

2017年11月08日(三) 03:30　Tweet

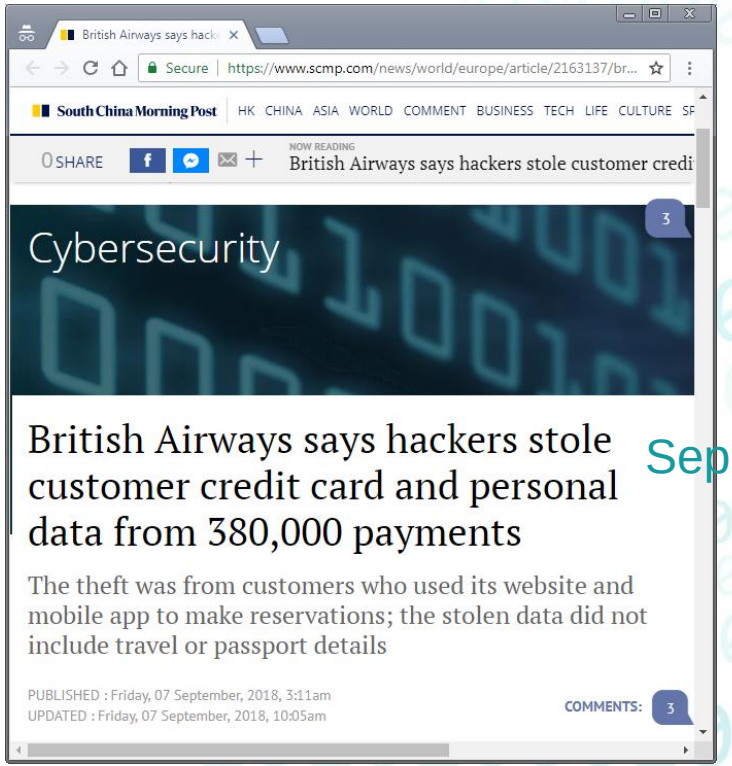
黃建達中指今次是本港首次有旅行社的電腦系統被黑客入侵。（資料圖片）　1/2

縱橫遊電腦系統客戶數據遭黑客入侵及勒索，是本地旅遊業首次發生同類事件，備受業內人士關注，多間主要旅行社均嚴陣以待，防止成為下一個受害者。業界均表示一直有加強電腦系統保安，會再次提醒職員切勿打開不明來歷的電郵及下載可疑軟件，並會為客戶資料進行加密及備份。

根據旅遊業議會資料顯示，今次是首次有本港旅行社電腦系統遭黑客入侵，是次旅議會主席的嘉泰旅行社董事總經理黃建達表示，旅議會相當注重業界電腦保安工作，今年已舉行兩至三次講座，又設立基金供有需要的旅行社申請，以提升電腦保安。

黃建達補充，嘉泰本身亦一直委託星視公司的電腦系統保安，經常作出更新，又一直提醒同事不要打開不明來歷電郵，以及不要隨意下載免費程式，他相信今次只是個別事件，可喚起業界的關注。

兼署華旅遊總經理李振庭形容，電腦黑客無孔不入，連外國政府機關亦給入侵，可謂「冇得擔心」。



Sep 2018

Multiple Layers of Defense

Digitization has transformed our world. How we live, work, play, and learn have all changed. Every organization that wants to deliver the services that customers and employees demand must protect its network.

Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

Protection at Edge

Anti-DDoS

Can be appliance or cloud based solution

Another Firewall

Preferably different brands

Segregate Internet facing applications from Internal systems

Internet facing systems

Corp Network

Firewall

To protect internal systems from outside world

Internal systems

Hosted Based Firewall

Installed on the specific server

Wireless Security

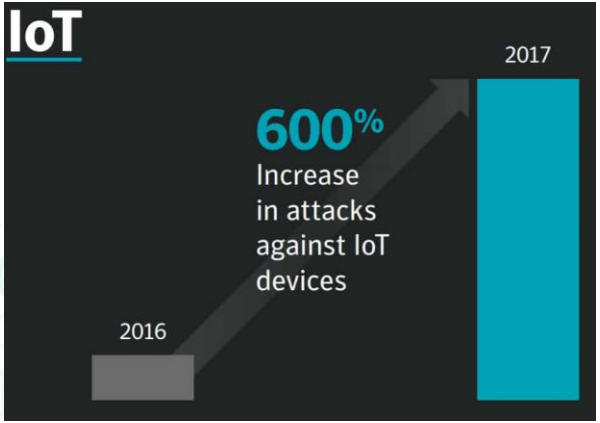
Two driving forces

Open up your network

Vulnerable to attack

Wireless technology opens up your network to the air.

Hackers do not need to have a cable connected to your corporate network.

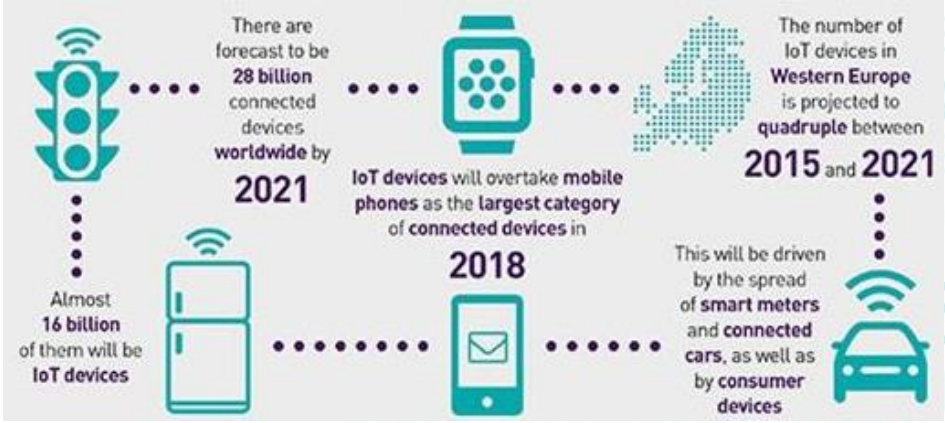


Explosion of IoT

More devices

Explosion of Smartphone and IoT devices increases the security threat to Wireless Network.

These devices are not designed with strong security protection.



Wireless Security

Best Practices

- Use strong authentication (e.g. WPA2-Enterprise)
- Set the SSID invisible
- Restrict access to designated devices
- Do not expose critical systems to WiFi network (if really necessary, implement 2-factor authentication)

Endpoint Security

AntiVirus

Anti-malware

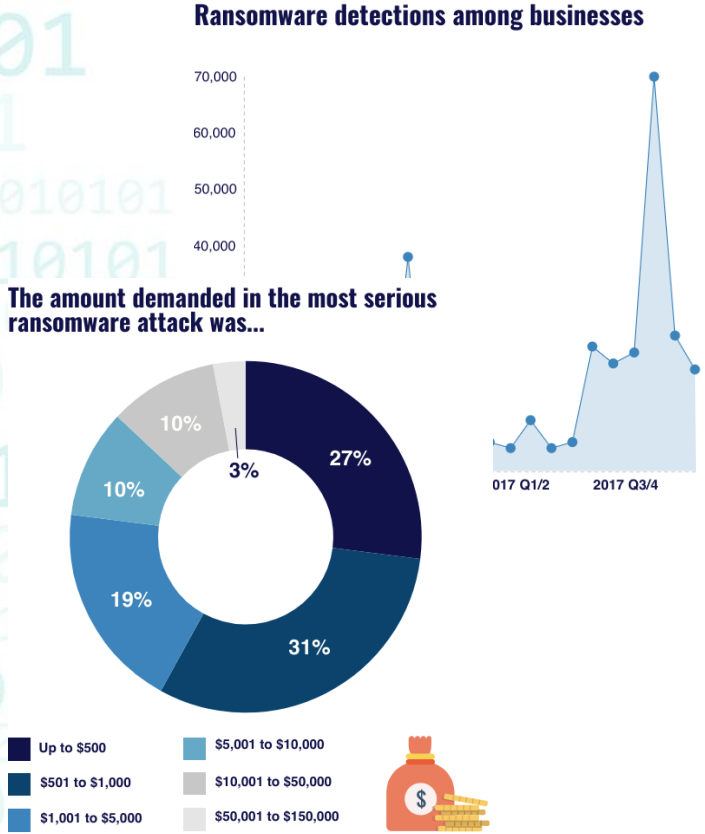
Patch Management

Personal Firewall

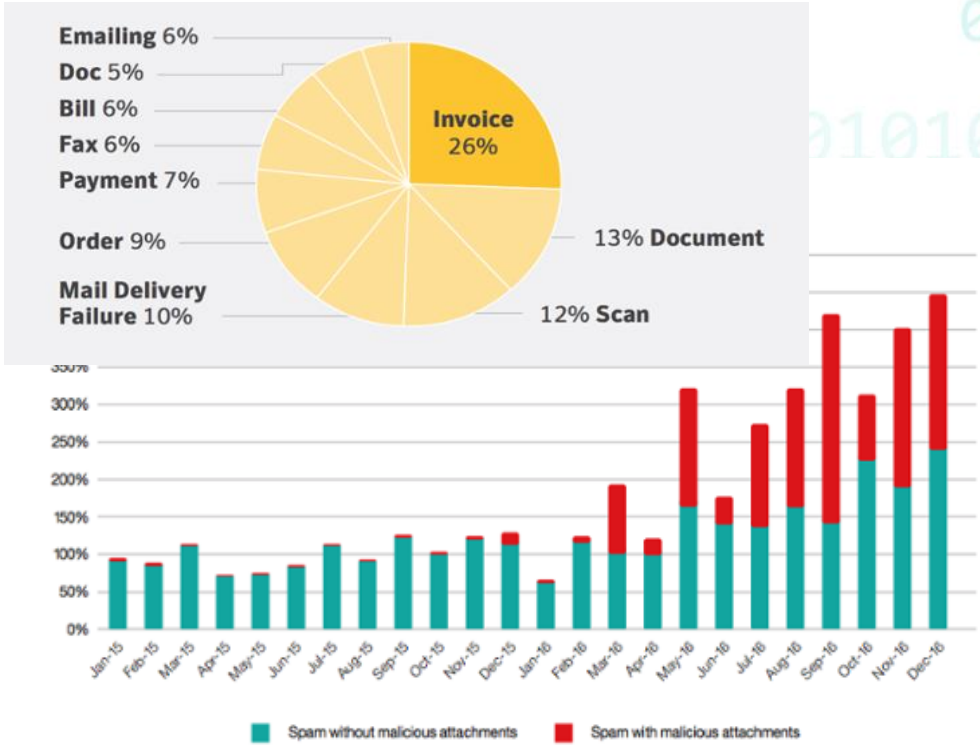
Network Access Control

Email Security

Businesses are seeing more malicious emails flooding their inboxes



Source: Symantec 2017 Internet Security Threat Report (ISTR)



Source: IBM Threat Intelligence Index 2017

Email Security

Education is the most important thing

- Watch out for phishing emails
- Never open unexpected attachments without scanning
- Use strong passwords that are unique
- Scan all emails for viruses and malware
- Use a robust spam filter

Operations Consideration

Privilege Password Mgmt

- Using strong passwords
- Exercise split password control
- Use password vault

Patch Management

- Ensure critical equipment are under maintenance
- Check the update and patch

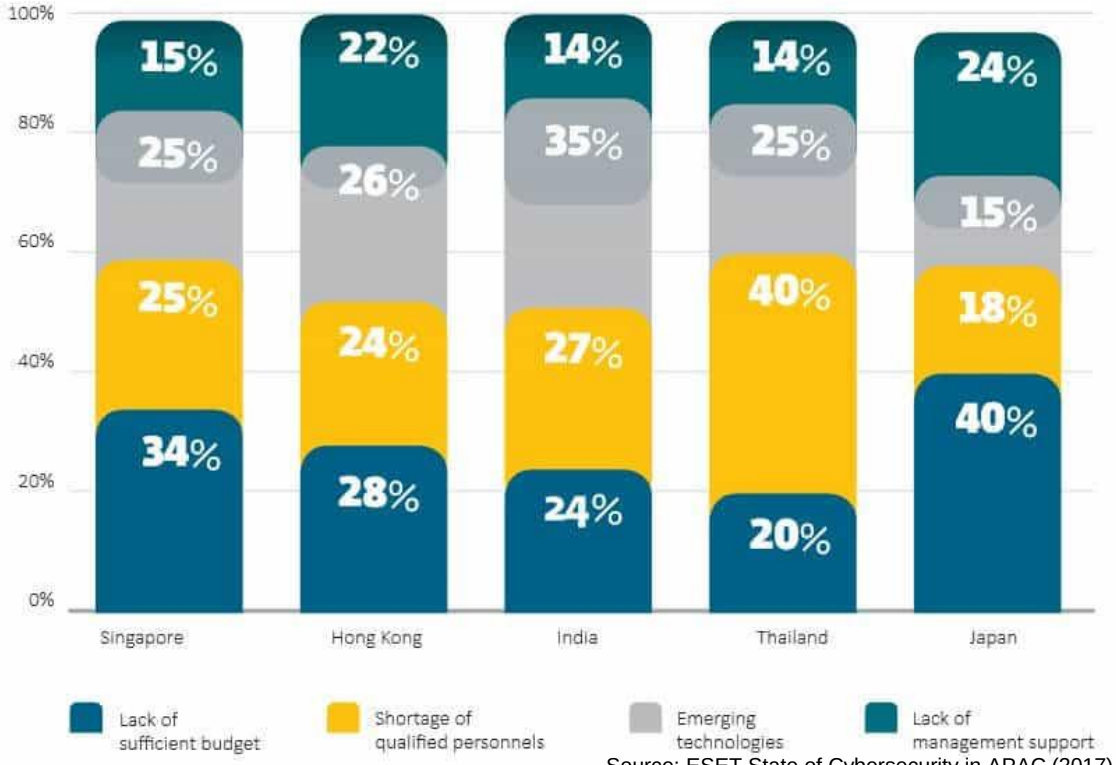
Inventory/Configuration

- Maintain configuration document
- Maintain connection diagram
- Backup of configuration

Backup

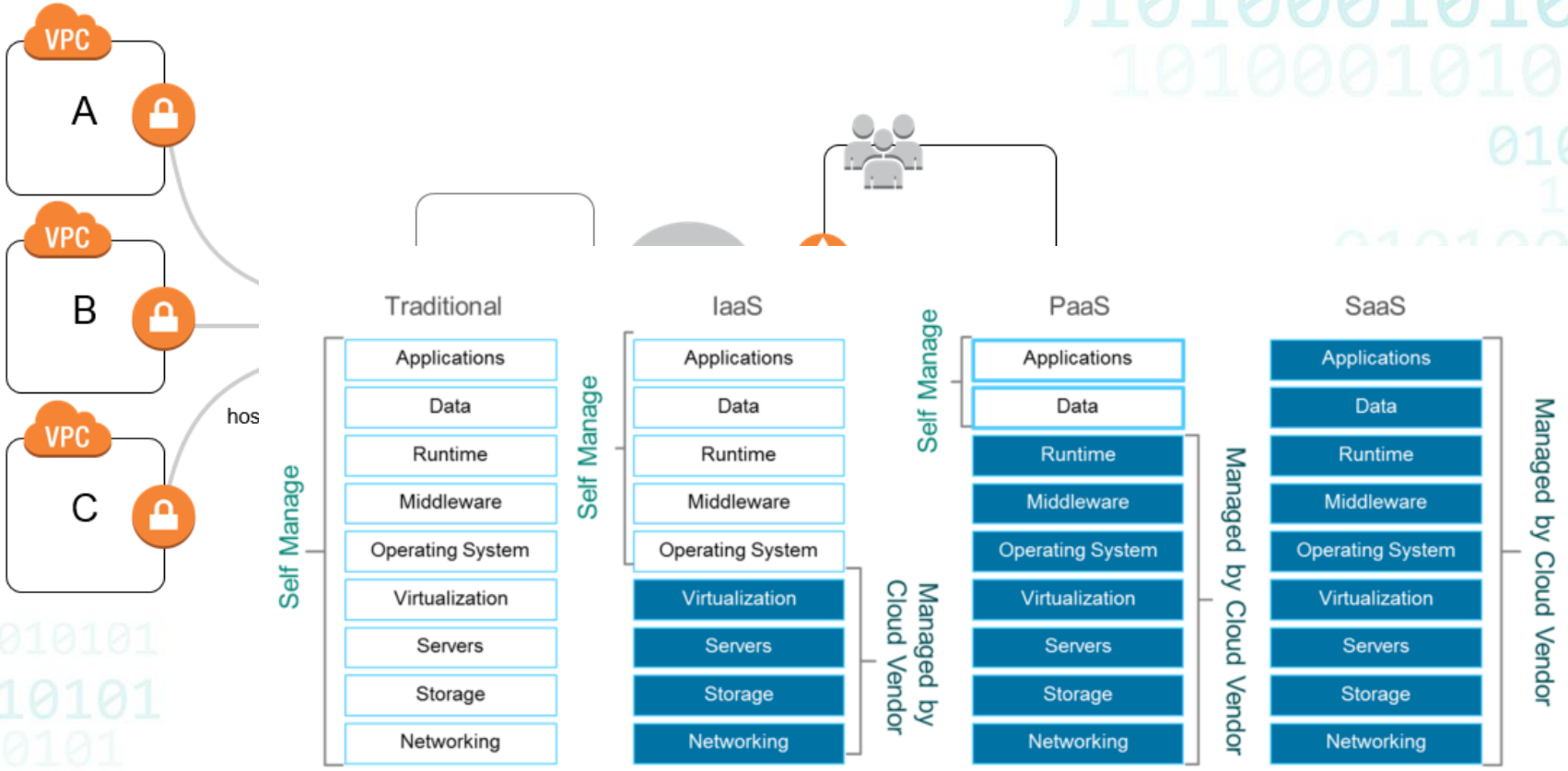
Backup critical data and configuration parameters

Challenges faced by SME



Source: ESET State of Cybersecurity in APAC (2017)

Cloud Security Consideration



Cybersecurity – Next big topic

Key findings

87%
of respondents say they need up to 50% more cybersecurity budget.

77%
of respondents consider a careless member of staff as the most likely source of attack.

48%
do not have a Security Operation Center, even though they are becoming increasingly common.

36%
of boards have sufficient cybersecurity knowledge for effective oversight of cyber risks.

12%
feel it is very likely they would detect a sophisticated cyber attack.

63%
of organizations still keep cybersecurity reporting mostly within the IT function.

57%
do not have, or only have an informal, threat intelligence program.

89%
say their cybersecurity function does not fully meet their organization's needs.

Source: EY

Key Take-away

Security is a never-ending investment

You will never see the benefit until one day you are attacked

There is tradeoff between security and performance/efficiency

Keep learning!

Thank you