Cyber Risks and Governance Post-Covid19

Anthony Lim

Director, CSCIS.org

Singapore

28Aug2020

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES
CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Prolog

Q: Who is responsible for accelerating digital transformation in the organization?

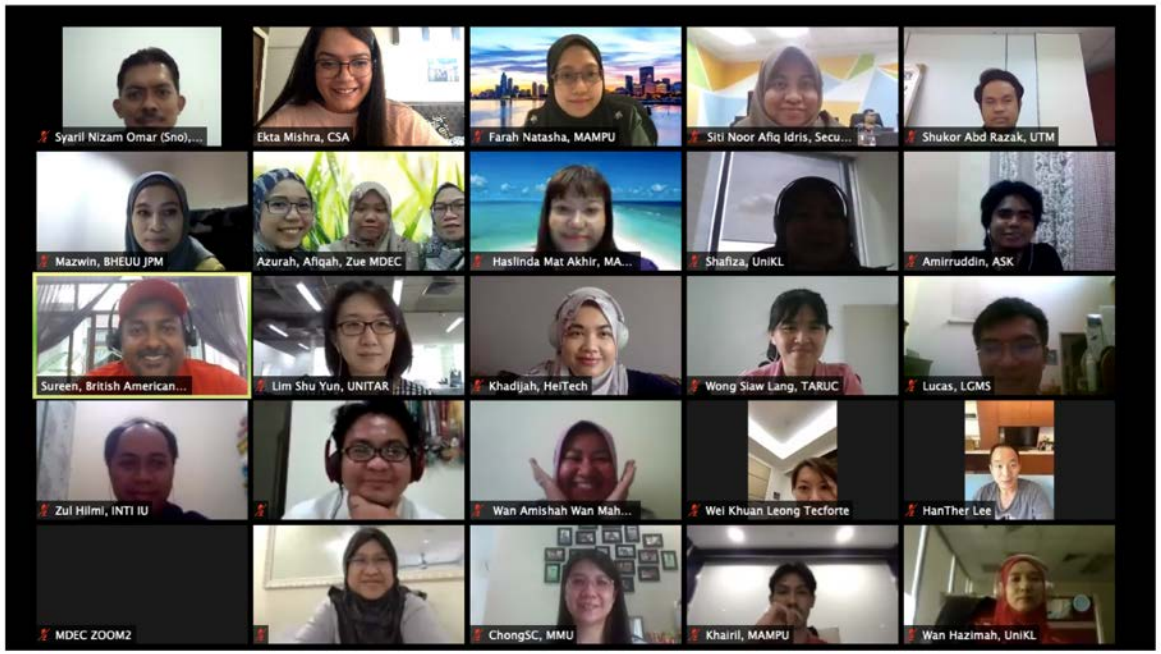
A: **(a) CEO**

(b) CFO

(c) CIO

(d) COVID19 **( )**

Covid19 and post-Covid19 – The “New Normal”?!



Suddenly Everyone

- **lockdown**
- **Zoom**
- **VPN**
- **WFH**

zoom

Microsoft Teams

Cybersecurity Talks | Working from home, is it safe and secure?

Guest Speakers:

Tengku Shahrizam
Cybersecurity Sales Manager, Cisco Malaysia
Cisco Systems

Steven SIM Kok Leong
Vice President
ISACA Singapore Chapter

Mohammad Firdaus Juhari
Vice President, Cyber Security
Khazanah Nasional Berhad

Cedric Warde
Director of Digital Trust & Cybersecurity Product Management, ICT Business
du

Azrul Shahmi bin Mansur
Assistant Vice President, Data Centre Facilities Management
CSF Advisers Sdn Bhd

Moderator:

Javed Abbasi
Principal, Digital & Cybersecurity Specialist
GISBA

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES
CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Cyber Risk Management – Some Questions

1. Have roles and responsibilities relating to cybersecurity been clearly defined and communicated at every level of the organization up to the CEO and Board?

2. Do business leaders understand the cybersecurity risks they are accepting?

3. Are technology solutions designed, integrated and operated with security and privacy in mind?

4. Does the business incentivize the adoption of secure-by-design-and default practices on the businesses and products in which it invests?

5. Are third-party risks managed effectively?

COVID19:

TOP TEN

Most worrisome risks for your company

WORLD ECONOMIC FORUM

COVID-19 Risks Outlook A Preliminary Mapping and Its Implications

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Poll # 1 – Post Covid-19, how your customer business has changed?

- Spurt in **usage of cloud services** on the back of **work-from-home.**
- Stay-at-home has become the **new normal.**
- Adoption of public cloud and remote computing **will accelerate** coming out of the current pandemic, increasing complexity for enterprise and limiting the effectiveness of traditional perimeter-based network security.
- More security lapses, inducing risks of hacking and phishing emails.
- Usage of own device that are not properly configure raise possible security breaches for enterprise
- Faster shift to Zero Trust architecture, nothing is implicitly trusted.
- Infrastructure will remain Hybrid and the Network still important.

Some Cyber-security Threats Arising from Covid19

1. Malicious or badly-written Covid-themed mobile apps
2. Weak VPNs.
3. Covid-themed phishing emails and messages.
4. Attacking home routers.
5. Attacking Zoom and other web-conference platforms.
6. Attacking organization's branches
7. Attacking an enterprise's supply-chain and eco-system business partners (suppliers, sub-contractors, outsourced service providers)
8. Attacking work-related social media
9. Attacks on national critical infrastructure and "smart" assets
10. Security solutions mis-configuration in haste to keep up with re-jig

Covid19 – Some Other Cyber-related Risks

1. C-executive imposter fraud exploiting social distancing
2. Insecure remote connections to the office
3. Increased personal use of company devices
4. Employees under financial stress or job uncertainty may pose an inadvertent risk as insider threat
5. Confidentiality at home
6. Covid-theme Phishing attacks
7. Employee "Zoom" fatigue

Covid19: Immediate Impact Organizations May Face

Maintaining business operations will be prioritised in a culture of crisis.

Priorities will shift as many organisations prepare for, or experience, significant financial and operational challenges. This may lead to IT and cyber security being deprioritised, with budgets being cut or at least their future being uncertain and hiring freezes put in place. This may affect planned security and IT improvement programmes and could delay important activities, including those that make organisations more resilient to cyber threats.

Higher numbers of the workforce will be absent and efficiency may decrease.

As COVID-19's impact on society increases and infection rates rise, higher numbers of the workforce are likely to be absent, especially as we head into peak periods of infections. Those who remain are likely to be less effective due to an increase in additional pressures, or general worries about the situation.

Critical suppliers will be disrupted, potentially interrupting crucial security activities.

Organisations' supply chains will also be impacted and this may lead to disruptions in service provision. This is likely to include critical elements of the security supply chain, for example, outsourced Security Operation Centres, patching, and firewall management teams.

Organisations will become increasingly reliant on remote access technology, including technology their employees are not familiar using.

As organisations move away from their physical premises, and become increasingly reliant on remote access technology, any disruption caused by cyber security attacks or IT outages will have a significantly greater operational impact. Furthermore, the usual manual or physical workarounds used to overcome these issues may be unavailable.

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Covid19: Immediate Impact Organizations May Face

(continued)

The workforce will rapidly shift to remote working and require technology to support this.

Shifting to remote working at both scale and pace is likely to cause significant impact, changing both IT infrastructure requirements and the attack surface. This will cause significant pressure on security teams, who may be refocused to support general IT operations, or to rapidly modify processes and technologies to adapt to changing risk.

Organisations should take three key actions to mitigate these emerging risks:

1. Secure their newly implemented remote working practices.
2. Ensure the continuity of critical security functions.
3. Counter opportunistic threats that may be looking to take advantage of the situation.

SUSS Singapore University of Social Sciences | CSCIS Centre for Strategic Cyberspace + International Studies

Enterprise Digital Transformation – CyberSecurity Considerations

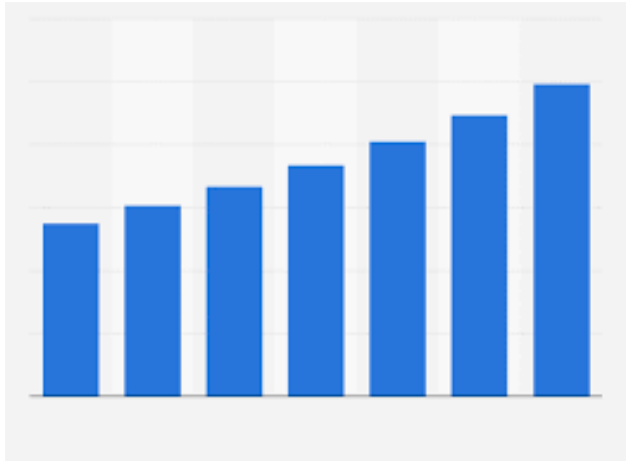
Digital Transformation involves deploying information technologies (systems, applications, services) not usedcBefore in the organization – BYOD, Mobile Applications, Cloud Services, IOT, e-commerce, e-payments, FinTech … it is imperative that the enterprise cyber-security considerations extend to cover all these.

1. Prioritizing Cloud Security
2. Use Zero Trust Access Protocols
3. Stay Up-to-Date on Data Protection Regulations
4. Secure Web Services
5. Secure Applications (including Mobile Apps)
6. Strengthen Wireless Connections (whether WLAN or WAN)
7. Extending Security to Remote Locations

Covid19 – Enterprise Cyber-security Spending Hot-spots

McKinsey & Company

1. Perimeter and remote access security, 2FA.
2. Next-generation identity and access controls
3. Automation (use of MSSP, SOAR).
4. Security training and staff awareness.
5. Security for trusted third parties.



SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Covid19: How Businesses can Respond to Cyber-Threats

- **Understand the threats to your organization.**
- **Provide clear guidance and encourage communication.**
- **Provide the right security capabilities.**
  - ✓An ability to securely connect users to their business-critical cloud and on-premise applications, such as video teleconferencing applications increasingly relevant for remote work environments
  - ✓Endpoint protection on all laptops and mobile devices, including VPN tools with encryption
  - ✓An ability to enforce multi-factor authentication (MFA)
  - ✓An ability to block exploits, malware and command-and-control (C2) traffic using real-time, automated threat intelligence
  - ✓An ability to filter malicious domain URLs and perform DNS sinkholing to thwart common phishing attacks

Covid19: Enterprise Cybersecurity operations suddenly facing tremendous challenges

1. **Working from home** has opened multiple vectors for cyberattacks through the **heightened dependency on personal devices and home networks.**
2. **Social engineering** tactics are even more effective on a distracted and vulnerable workforce.
3. Security Operations Centers (SOCs) have been designed to look for anomalous behaviors; today, **SOCs are operating with impaired visibility because everything looks anomalous**.
4. **Critical business assets and functions** are significantly more exposed to opportunistic and targeted cyberattacks by criminal organizations and nation states seeking to exploit vulnerabilities and plant seeds for future attacks.
5. **Public-sector services such as hospitals and healthcare services are under acute pressure** and have been hit particularly hard by new types of ransomware aimed at disrupting connectivity and denial-of-service attacks.

Some key Covid19 Cyber Risks for Banks

1. The staff (inadequately-secured) remote connection challenge
2. Trader surveillance interrupted (inability to comply)
3. Priorities for the future

(a) Rethink Remote Access Security Management and Enablement

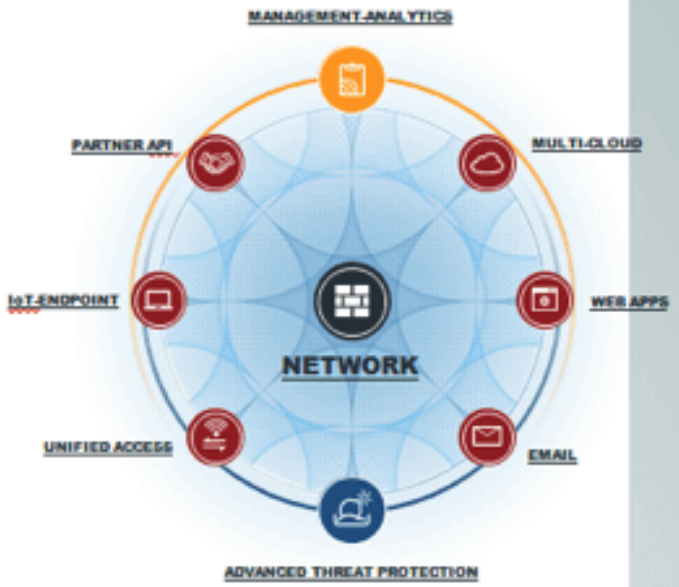
with levels of remote working likely to remain higher than they were pre-COVID-19, banks may need to 'reset' some of their protocols and policies around access management, finding ways to increase flexibility without compromising security. They are also likely to look for more secure video conferencing services.

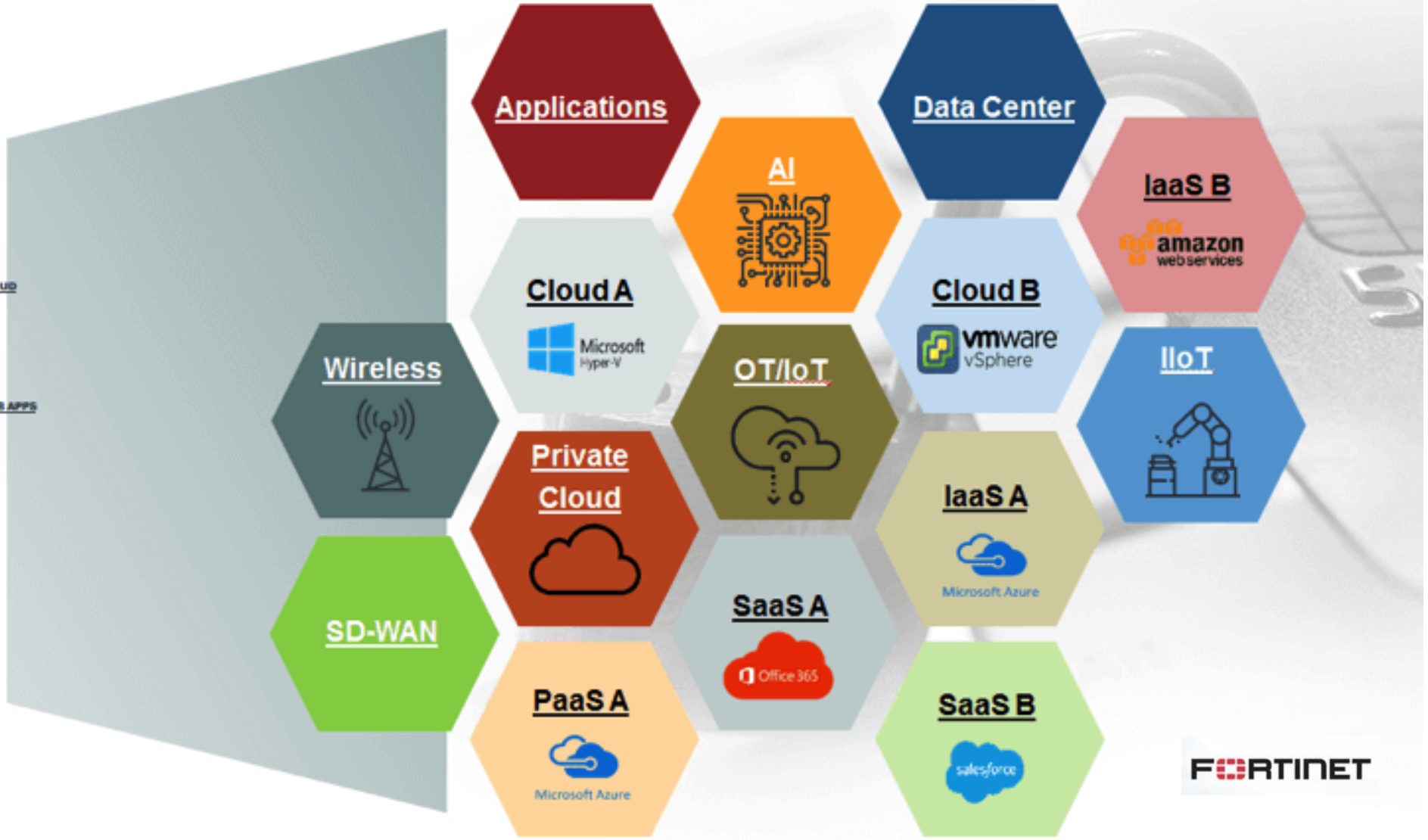
(b) Increase in Dependence on Publlc Cloud Services

in a lockdown and other emergency situations, with public cloud, patch management and other security features can automatically run remotely (rather than rely on incumbent on-premise equipment or private cloud and self-management herein).

Digital Transformation – Many New Technologies to Secure

Security of information must be addressed in lock-step with DX going forward. Modern network defenses must safeguard data across the extended network of the organization. It must protect data across systems, devices, and cloud—including emerging technologies that are not yet in the network. In times of rapid change, effective security must anticipate what's to come in the foreseeable future.

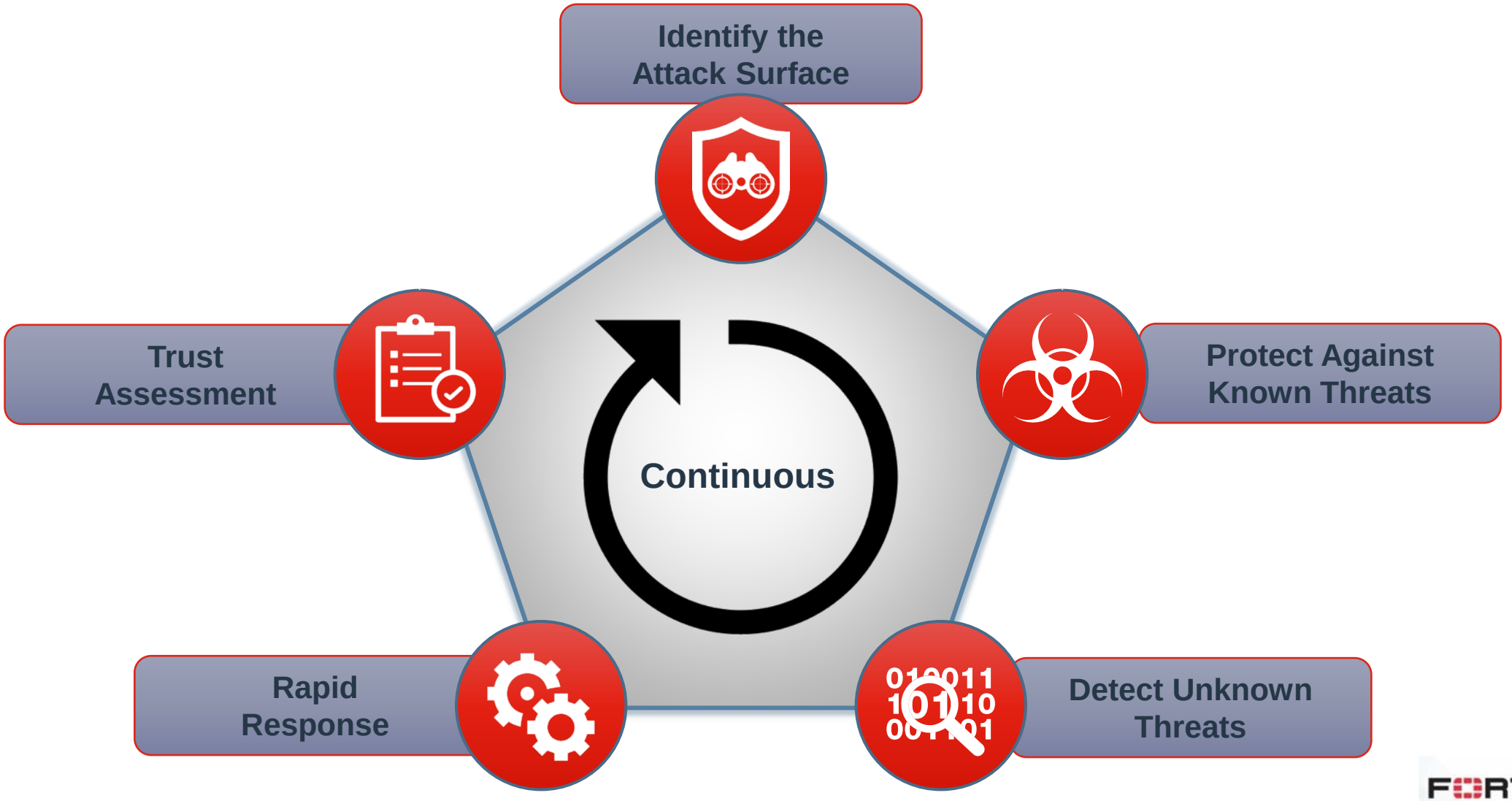




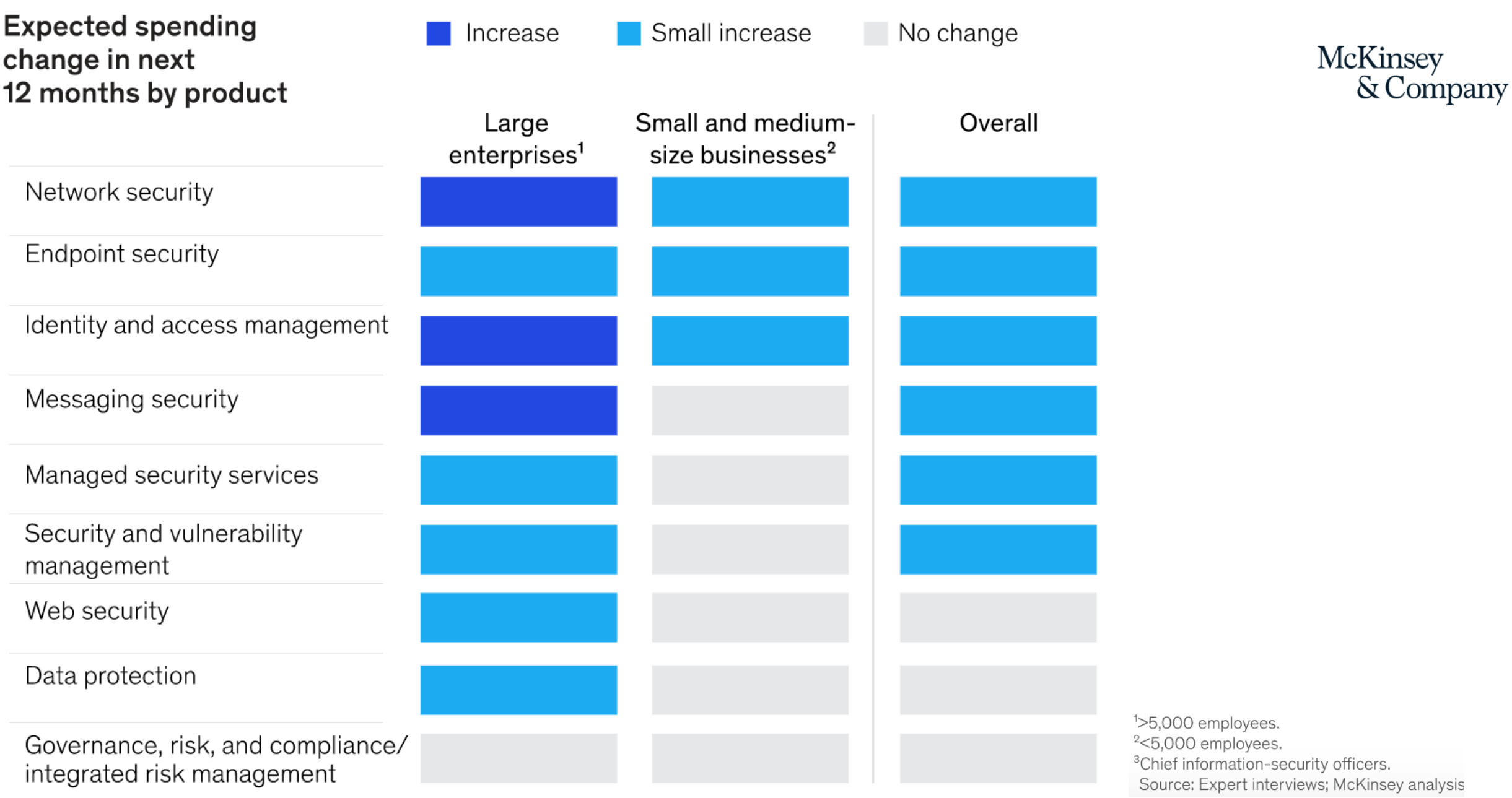
SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

FORTINET

Security Framework for Cyber-resilience



Expected spending change in next 12 months by product



McKinsey & Company

[1]>5,000 employees.
[2]<5,000 employees.
[3]Chief information-security officers.
Source: Expert interviews; McKinsey analysis

- >70% of CISOs[3] and security buyers believe budgets will shrink by end of 2020 but plan to ask for significant increases in 2021
- Product spending reflects CISOs' need to address pandemic-era business conditions, including safeguarding remote workers from heightened attacks

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS

Covid19: Enterprise Cyber-Resiliency Imperatives

SECURITY
SOLUTIONS FOR ENABLING AND ASSURING BUSINESS
Magazine

1. Secure Remote Networking

Post-COVID-19 organizations will re-examine their technology stacks to integrate solutions that more securely support a remote workforce. This includes scrutiny of digital collaboration tools that have become a mainstay of remote working.
Widespread employee usage of unsecure messaging and conferencing apps left many organizations open to significant security and compliance risks

2. Cyber-security Training and Education

3. Moving to a Zero-Trust Operational Model

4. Strengthen collaboration.

Per KPMG & WEF “strengthen eco-system-wide collab

Zero Trust –
* Do not automatically grant access for Anything n everything To network or other IT assets, verify First, whether f rom within or outside Of network perimeter.

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Covid19: Cyber-security Leadership Principles

1. Foster a culture of cyber resilience

   Incident Response, Disaster Recovery, Business Continuity

2. Focus on protecting the organization's critical assets and services

3. Balance risk-informed decisions during the crisis and beyond

4. Update and practice the organization's response and business continuity plans as business transitions to the “new normal”

5. Strengthen ecosystem-wide collaboration

Conclusion: Leading Cyber-security In The New Reality

KPMG

1. **Foster a culture of cyber resilience.**
2. **Focus on protecting critical capabilities and services.**
3. **Balance risk-informed decisions during the crisis and beyond.**
4. **Update and practice your response and business continuity plans.**
5. **Strengthen ecosystem-wide collaboration.**

Deloitte.

- *Some considerations per Deloitte*

1. Supporting safely working from remote locations.
2. Identifying and countering phishing schemes.
3. Improving enterprise-wide cyber defense strategies.

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

CYBER RISKS AND GOVERNANCE POST-COVID19

Thank You / Q&A

Anthony Lim

Director, CSCIS.org

Singapore

28Aug2020

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES
CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES