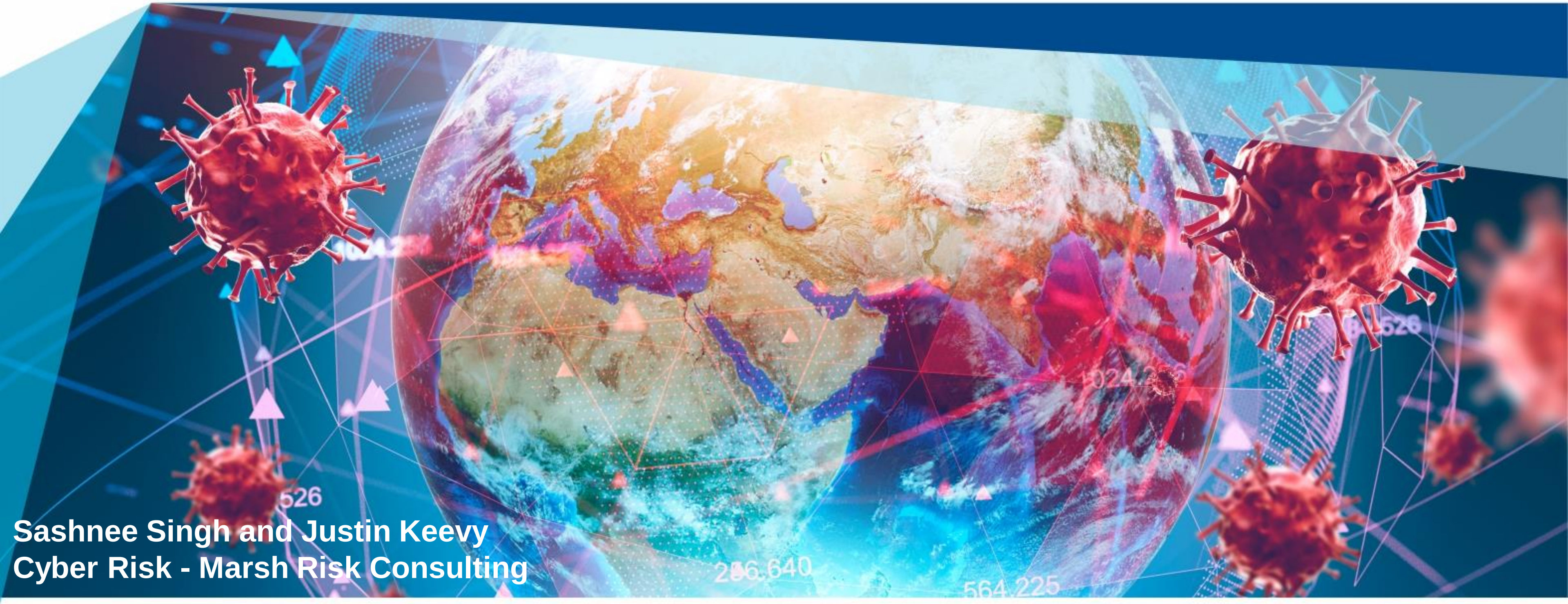
MARSH RISK CONSULTING

INSURETALK VIRTUAL CONFERENCE
THE COVID-19 PANDEMIC AND CYBERSECURITY

14 APRIL 2020



Sashnee Singh and Justin Keevy
Cyber Risk - Marsh Risk Consulting

Some Alarming Statistics
Hackers are taking advantage of the situation to attack

- Coronavirus has generated the highest volume of cyberattacks recorded in years.
- 400% increase in phishing attacks
- Hackers hit 300,000+ devices in SA in 1 week as more people started to work from home
- 34% of South African computers may be at risk of infection without users' knowledge as they rely on an outdated or unsupported version of Microsoft Windows operating system (OS).
- More than 4,000 Coronavirus-related websites have been registered since January (3% domains reported as malicious; 5% suspect)
- Fake apps and domains related to popular services like Zoom or Google Classroom are also being used to affect users and organizations.

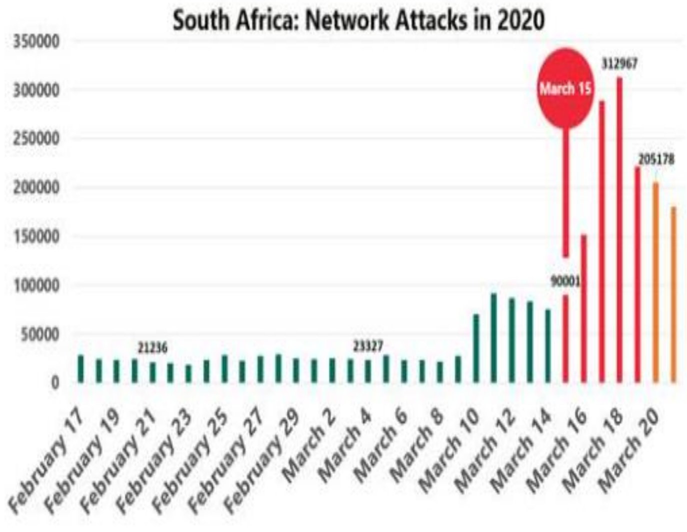


Image: Kaspersky

Sources:
ITWeb; Kaspersky
https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains
https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains

The Pandemic has created the perfect storm for Cybercriminals
Some Recent Cyber Scams

Hackers use a live COVID-19 map to spread the AZORult malware, which steals passwords, payment card information, cookies, and other sensitive data

Fabricated WHO recommendations, claiming that virus is now airborne & that new cases have been confirmed in the victim's vicinity. Attached to the message is a file named "SAFETY PRECAUTIONS", which looks like an MS Excel™ document, but is in fact an executable file (.exe)

A claim that the UK and Chinese governments have been covering up details about a new vaccine. Clicking on the attached document leads to a spoof Web page designed to collect login details

Marriott suffers a second security breach, exposing 5.2 million guest data

(https://thehackernews.com/2020/03/marriott-data-breach.html)

[EEUU 30/03] COVID-19: Hackers begin to exploit Zoom's resounding success to spread malware

(https://thehackernews.com/2020/03/zoom-video-coronavirus.html)

Hackers created thousands of coronavirus-related sites (COVID-19) as bait

Organisations are adjusting to new ways of working

They are taking decisive actions to continue operating during the crisis

Enabling remote access for a large number of contributors and third parties (VPN, TeamViewer, AnyConnect, Remote Desktop, etc.)

Permissions to bring desktop computers to employees' homes

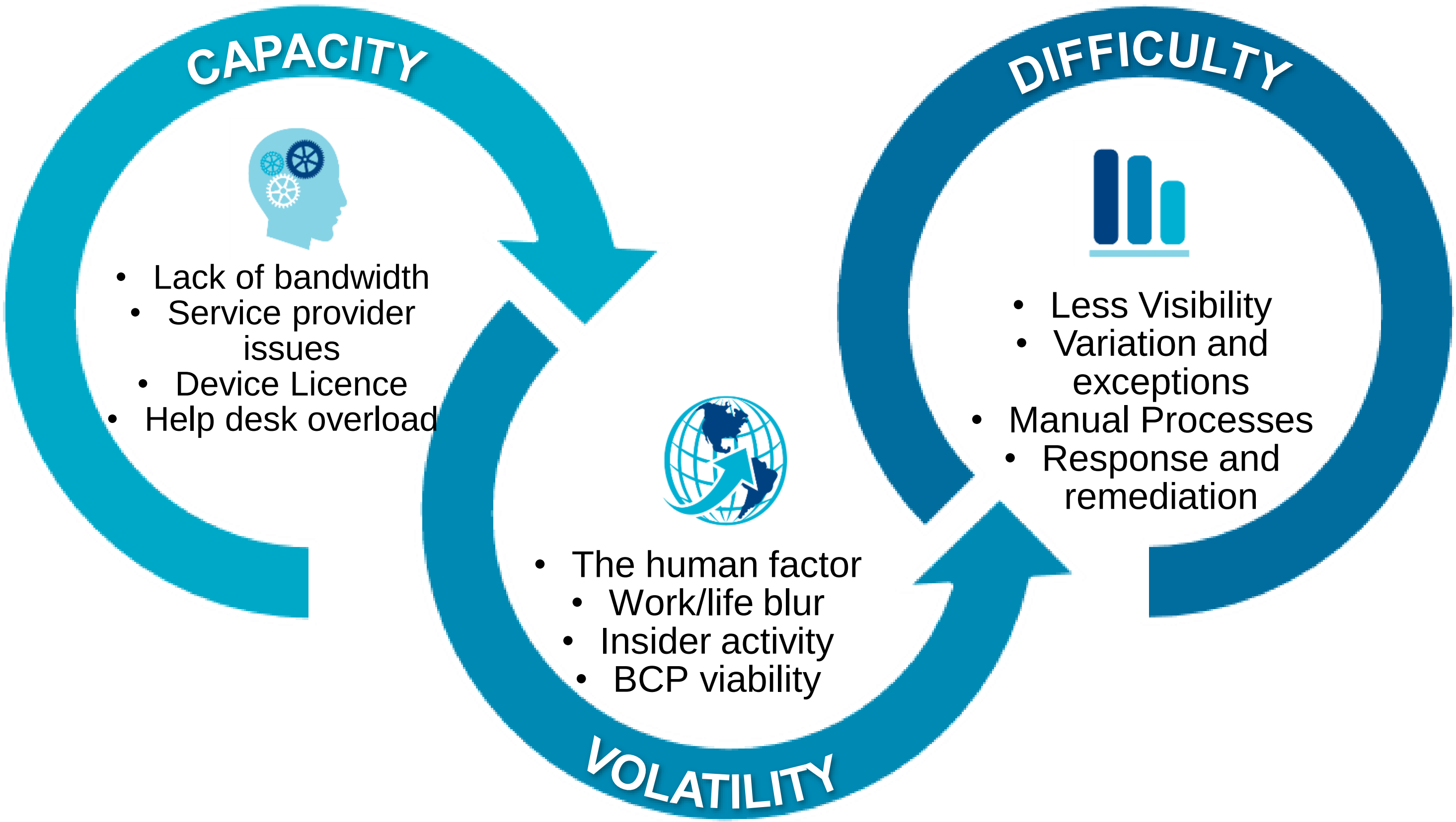
Permissions for connections to personal computers

Exposure of internal services, in the process of testing or that have not been adequately insured (e.g. internal applications, email, etc.)

Disabling security controls (e.g. double factor authentication, restriction by geolocation, etc.)

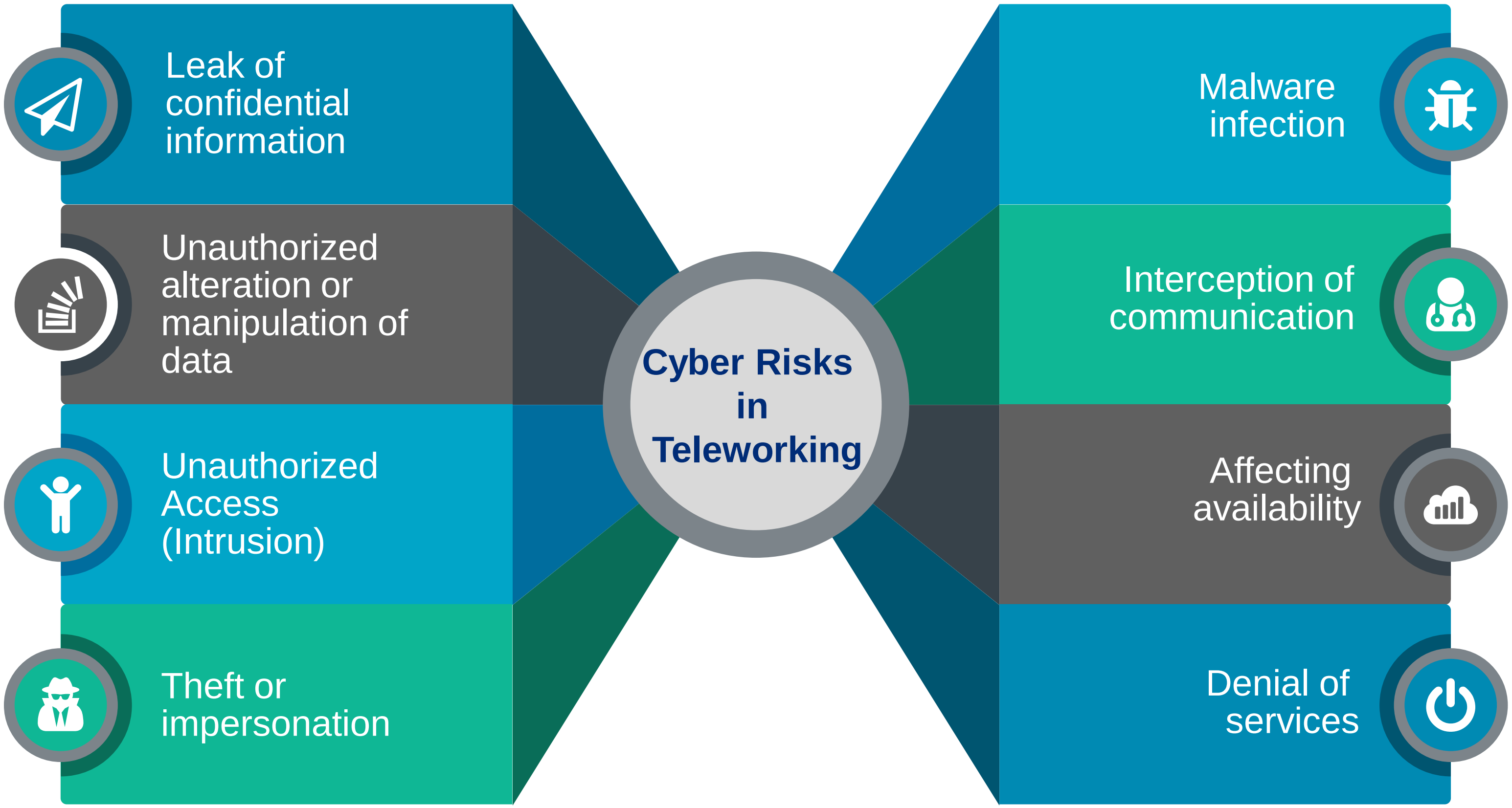
Use of videoconferencing facilities, e.g. Zoom

Managing Cyber Risk at a ‘Distance’
Security teams are struggling with managing these



Managing Cyber Risk at a ‘Distance’

With remote working, some Cyber Risks Have become more Relevant



Has your organisation performed cyber risk assessment for remote working?

Awareness and training

Key concepts related to the cyber-risks of remote work to which collaborators are exposed.

Security Architecture

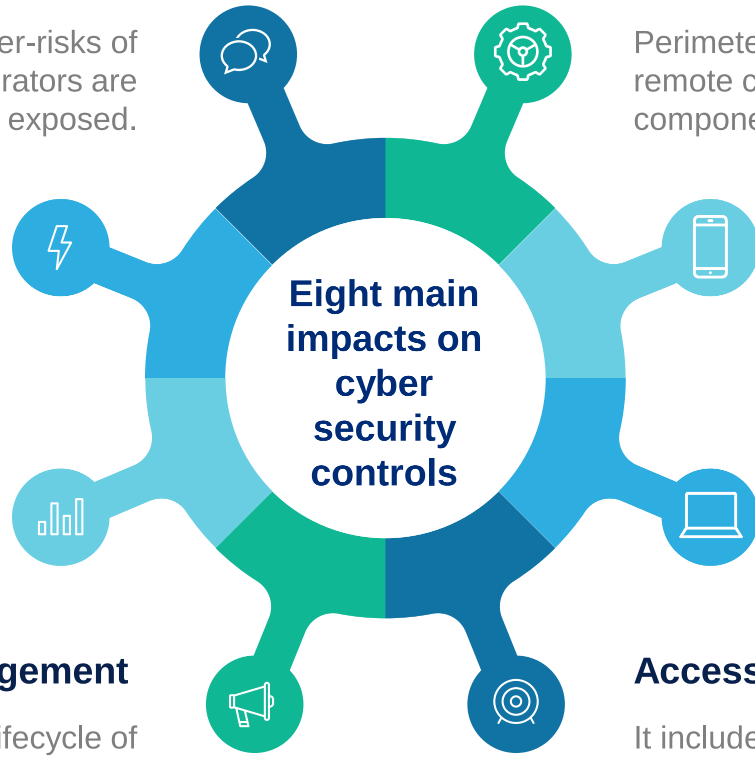
Perimeter security and remote connection components.

Response to Cyber Incidents

Implemented and tested capabilities for response to a detected security event.

Mobile devices

Security settings on mobile devices.



Monitoring Security events

Critical features for timely detection of security incidents.

Work Stations

Security aspects of users' workstations.

Vulnerability management

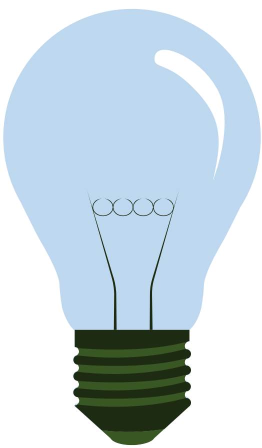
Critical aspects related to the lifecycle of vulnerabilities in the organization.

Regular patching

Access Management

It includes process-related aspects that ensure that only authorized users have relevant access. VPNs, MFA

In Conclusion
Three Key Takeaway Points

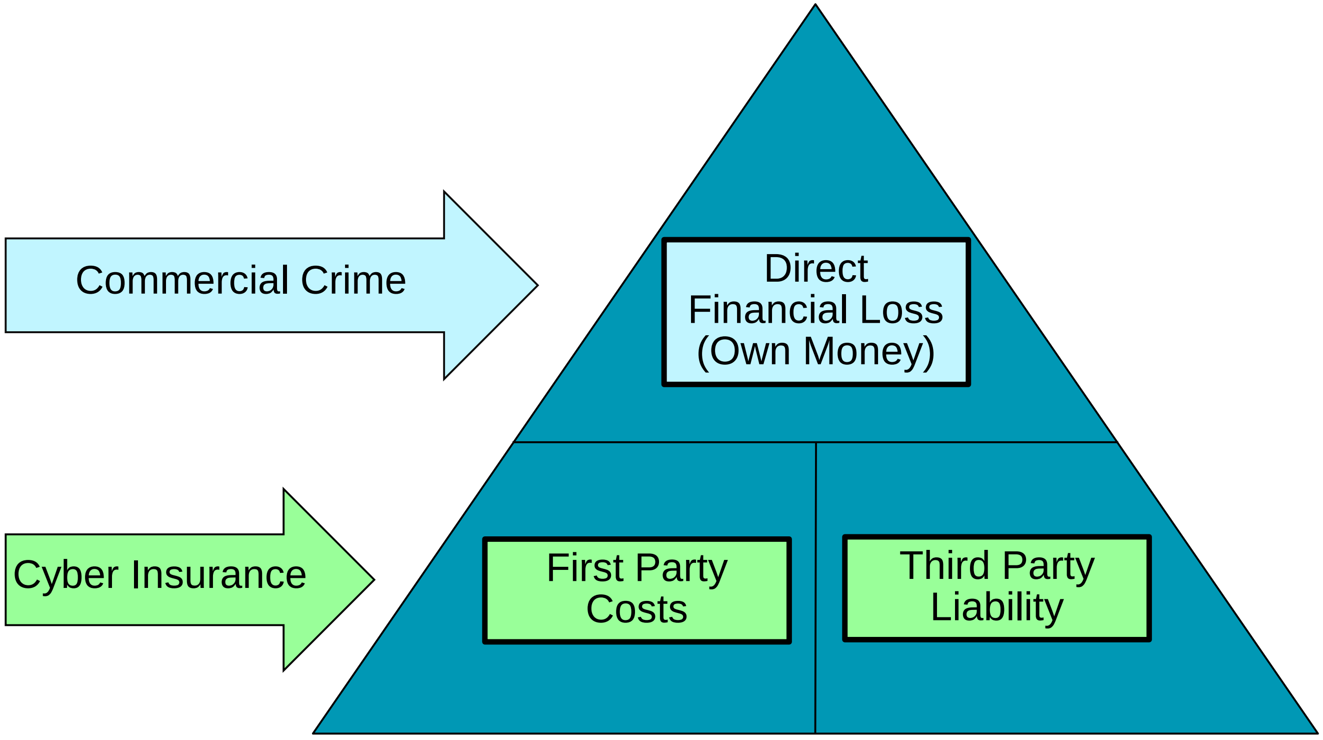


1. The COVID-19 crisis is likely to stay with us for a while. A cyber risk assessment for teleworking is key to ensure that we are secure when working from home

2. Re-enforcing **security awareness** is key to limiting cyber attacks

3. Develop COVID-19 specific playbooks and adapt **disaster recovery plans** to current operational context and aim to initiate plans to cater for a worst-case scenario

Difference between a Commercial Crime Policy and a Cyber Insurance Policy



Cyber Risk

Coverage provided under a Cyber Risk Insurance Policy

A) First Party Costs

- A1 Incident Response
- A2 Network Interruption
- A3 Extortion

B) Legal Liability

- B1 Privacy Regulatory Fines and Penalties & Legal Liability
- B2 Crisis Management and Notification Costs
- B3 Digital Media

MARSH RISK CONSULTING

An authorised financial services provider

FSB Licence no.: 7784

Registration no.: 1993/005898/07

Directors: MS Duncan, S Fatouros, K Groenewald, M Pienaar