Institute
and Faculty
of Actuaries

IFoA COVID-19 Action Taskforce (ICAT) Cyber Security Workstream

Cyber Security Implications of COVID-19 for Companies

10.1.2021

Acknowledgements

We would like to thank all the members of the ICAT “Cyber Security Implications of COVID-19” volunteer group who have provided valuable insights and contributions in generating and reviewing output:

- Aastha Bajaj
- Miriam King
- Hazel McNeilage
- Atong Mu
- Amal Nirmal
- Rushabh Shah
- Martin Snow

We would also like to thank Richard Campanha, Head of the IFoA Cyber Operational Risk Group, for peer review of this presentation.

If you have any questions please reach out to icatcyber@fastmail.com

What We Were Asked to Consider

What cyber related issues have arisen as part of the pandemic?

How much of this was predictable and were companies adequately prepared?

What needs to be improved going forward? (Not cyber insurance)

This document was produced by the ICAT Cyber Security Workstream to summarize the findings of a literature review conducted by the workstream during its research on the questions above.

This review focuses on the cyber implications of COVID-19 for companies in general.

A Few Quotes

“Greater than 6000 percent increase in coronavirus themed spam, March 11 to May 8 2020” IBM X-Force*

“20 000+ new vulnerability reports predicted for 2020, shattering previous records” Sky Box***

“The ‘Weaponization’ of COVID-19” AXA^^

“Work from anywhere. Cyber everywhere” Deloitte**

“Near seven fold increase in spear-phishing attacks, since the pandemic began” McKinsey, July 2020^

“96% of executives plan to adjust their cybersecurity strategy due to COVID-19”****

“Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19.”
Jürgen Stock, INTERPOL Secretary General ^^^

*’COVID-19 cyberwar: how to protect your business’ by IBM   ** Title of a Deloitte 2020 paper *** ‘2020 Vulnerability Trends Report’ by Skybox **** ‘Global Digital Trust Insights Survey 2021’ by PwC, 5 October 2020 ^ ‘COVID-19 crisis shifts cybersecurity priorities and budgets’ by McKinsey ^^’Operational Risks and COVID-19 ’ by AXA ^^^ Interpol report August 2020

Overview of Cyber Security Implications of COVID-19

IMPACTS OF COVID -19	CONSEQUENCES WHICH HAVE CYBER SECURITY IMPLICATIONS	CYBER SECURITY RISKS
Work From Home: Substantial increase in WFH, implemented very quickly; may well at least partially become permanent	• Increased use of video conferencing apps • Work may be done on employees' personal IT equipment • Employees connecting remotely to company networks • Employees not subject to normal oversight/may be subject to high stress • Sensitive organization data in employees' homes/potentially on their personal devices • Organization's normal policies, procedures and controls may be suspended/modified • Potential increased use of shadow IT by employees	• Exposure to security weaknesses of video conferencing apps (e.g., theft of confidential information, disruption of business conversations). • Compromise of organization's networks and/or systems and/or data through phishing and/or social engineering and/or attacks targeting insecure network connections or other weaknesses caused by changed working arrangements.
Other Employee Impacts	Workplace safety concerns, reduced working hours, salary reductions, furloughs and layoffs increase stress on employees and can lead to disaffected employees/former employees.	Increased insider threat Potential increase in hacker population
Supply chains/outsourcing relationships	Potential need to quickly re-engineer how supply chains/outsourcing relationships work	Increased exposure to the cyber weaknesses of suppliers/outsourcers, particularly if insufficient cyber related due diligence is done
Demand for and cost of products and services Potential for swift and substantial changes	May require a significant change in business model and materially change the company's financial position, either positively or negatively.	Reduced propensity/ insufficient bandwidth /inability to invest adequate time and resources in cyber security
Increase in pace of digitization of businesses	Greater dependency on systems and networks, including connectivity to 3rd parties	Increased attack surface; higher potential profits for hackers. Heightened vulnerability to attacks which involve systemic risks (e.g. telecoms providers; core telecoms infrastructure; cloud providers).

Types of Attacks

Types of attacks reported as having increased at least partly due to COVID-19 include:

Phishing

↑ nearly 700%^

This includes large quantities of COVID-19 themed phishing emails and lures as well as spear phishing*

Social Engineering

Seeks to exploit vulnerabilities due to employee stress, WFH, etc.

Malicious domains

COVID-19 related malicious domains and fake domains purported to relate to popular video conferencing services.

Vulnerabilities in employees connecting to company networks from home

Employee internet connections may not be secure.

Vulnerabilities in cloud applications

Over hasty cloud implementations

Vulnerabilities in unpatched generic systems (Microsoft, Citrix etc.)

Patching cadence may have reduced.

Ransomware

Once an attacker has gained access to a company’s system, ransomware is a popular method of attack. While verified statistics are hard to obtain, a 700% increase in ransomware attacks in 2020 has been cited by some industry experts.

^ McKinsey July 2020

* Targets senior management/directors

Threat Mitigants

Threat mitigants can be grouped into the following categories (not necessarily mutually exclusive):

- Policies and Procedures
- Employee Training
- Technological Mitigants
- Vendor and Other 3rd Party Management
- Business Continuity Planning
- Cyber Resourcing
- Cyber Insurance (not covered in this document)

Threat Mitigants:

Policies and Procedures

Work From Home Policies including:

- Devices usage: restriction/prohibition of use of personal devices for company business
- Accessing the company network (e.g. VPN; virtual desktop; multi factor authentication)
- Access to data and applications, including enhanced security policies for sensitive transactions (e.g. large payments)
- Data loss prevention
- Email security and web browsing
- Use, storage and disposal of confidential company information (physical and digital)
- Use of collaboration tools (Zoom, Teams etc.)
- Shadow IT
- Mitigate risk of slippage of standards that applied in a office environment and employee work arounds
- Review of any initial policy relaxations that were made at the outset of WFH.

Policy on Payment of Ransomware:

- Would this be contemplated?
- If so, under what circumstances?
- Regulatory implications
- Decision process
- Payment mechanism
- Payment may violate sanctions*

Other, including:

- Cloud policies particularly for sensitive data
- Modifications to policies for IT changes on critical systems (including possible freezes on changes if necessary)
- Technology governance.

**https://www.reuters.com/article/us-treasury-cyber-idUSKBN26M77U*

Threat Mitigants:
Employee Training

On what?

- Work From Home Policies and Procedures
- Video conferencing and other collaboration tools
- Phishing and social engineering
- Malicious domains related to COVID-19, video conferencing tools etc.
- The need to verify the authenticity of emails, voicemails, calls and texts
- Avoiding clicking on links unless absolutely sure they are safe
- Not revealing personal information
- Avoiding risky workarounds
- Upholding the same conduct standards as when in the office

Training content needs to be <u>dynamic</u> as threats evolve.

To Whom?

- All employees, directors and contractors
- Relatives of C-suite
- Particular focus on high risk users (e.g. Finance staff)

How?

- Employ a variety of methods: videos; quizzes; FAQs; reminders etc.
- Focus on <u>what to do,</u> rather than <u>what not to do</u>
- Relevant to the particular company
- Demonstrate senior management commitment

Threat Mitigants:

Technological Mitigants

Enterprise Architecture and Infrastructure:

- Minimize complexity of IT and security environments
- Privacy by deign
- Decommission insecure technologies (e.g. FTP; HTTP (SSL certification))
- Timely patching and updating for critical systems
- Email security controls
- System monitoring and analytics
- Fraud analytics/prevention
- Data Loss Prevention using AI
- Automated detection and response systems
- Cloud architecture and security

User Device Management for WFH:

- Device inventory
- Device encryption
- Remote wipe capabilities
- Up-to-date anti virus, threat detection and DLP software on all devices
- Regular back ups.

External Threat Monitoring

- Monitor company brand and disclosure of sensitive data on social media; pubic internet and Dark Net
- Subscribe to a threat monitoring service
- Industry collaboration

Connectivity/Access Management

- Virtual desktops (VNCs), or VPNs, including timely patching/updating
- Identity and Access Management (IAM) systems, including multi factor authentication; zero trust security
- Monitor all VPN and remote access logs
- Remote collaboration security

Threat Mitigants:

Other Considerations

Vendor and Other 3rd Party Management

Contracts

- Include cyber security requirements in existing and new contracts

Testing/Verification

- Initial and ongoing 3rd party security assessments

Collaboration

- Offer cyber tools and guidance to vendors and other 3rd parties
- Joint cyber resilience and monitoring with vendors and other 3rd parties

Business Continuity Plan and Incident Response Plan

- Update IRPs and playbooks for remote working
- Ensure critical IT staff and management can access systems remotely
- Back up plan if critical staff unavailable
- Alternative audio and video conferencing systems available for a crisis
- Test BCP and IRP with ransomware scenarios
- Test recoverability of back ups

Cyber Security Resourcing

With pressure on many corporate budgets, demonstrating efficiency and high value is key.

Review internal versus external resourcing.

Spend priorities*:

- Perimeter security
- Next-generation identity and access controls
- Remote access
- Automation
- Security training
- Security for trusted third parties.

**McKinsey: COVID-19 crisis shifts cybersecurity priorities and budgets July 2020*

Conclusion

What cyber related issues have arisen as part of the pandemic?

No notable new classes of cyber attacks but hackers very quick and effective in exploiting new access points (Work From Home), distracted/demotivated individuals, challenged business models and disrupted supply chains: resulting in elevated cyber attacks.

How much of this was predictable and were companies adequately prepared?

The speed of adoption of Work From Home and other business model/supply chain changes were difficult to predict; adequacy of preparation depended on existing business model and level of cyber maturity.

What needs to be improved going forward? (Not cyber insurance)

Required improvements vary depending on the existing level of cyber maturity and relate to one or more of: policies and procedures; training; technological controls; vendor and other 3rd party management; Business Continuity Plan/ Incident Response Plan ; cyber resourcing.

Bibliography

Cyber security threat levels rise as operations change - Grant Thornton, 29 May 2020

COVID-19-19-staying-cyber-secure – KPMG, 23 March 2020

Global Digital Trust Insights Survey 2021 – PwC, 5 October 2020

Managing the impact-of-covid-19-on-cyber-security – PwC, 20 March 2020

Securing the 'new reality' – KPMG, 12 May 2020

Seven ways to keep ahead of cyber attackers during COVID-19 – EY, 21 April 2020

2020 Vulnerability and Threat Trends Report – SkyBox https://lp.skyboxsecurity.com/WICD-2020-07-WW-VT-Trends_Reg.html

Cost of a Data Breach Report 2020 - https://www.ibm.com/in-en/security/data-breach

Cyber Insurance Claims Surge Amid COVID-19 - http://www.rmmagazine.com/2020/10/01/cyber-insurance-claims-surge-amid-covid-19/

COVID-19: Next Steps for Your Cyber Insurance - https://coronavirus.marsh.com/us/en/insights/research-and-briefings/covid-19-next-steps-for-cyber-insurance.html

Pandemic Poses a New Catastrophe Paradigm - https://www.guycarp.com/insights/pandemic-poses-new-catastrophe-paradigm.html

Cyber underwriters avoid COVID-19 exclusions even as ransomware concerns soar- https://www.theinsurer.com/viewpoint/cyber-underwriters-avoid-covid-exclusions-even-as-ransomware-concerns-soar/11769.article

Marsh - https://captivereview.com/news/increase-eb-cyber-captives/

Deloitte: The Acceleration of Digitization as a Result of COVID-19 July 30 2020

McKinsey: Safeguarding against cyberattack in an increasingly digital world June 2020

AXA: Operational Risks and COVID-19 June 16 2020

AXA Threat Intelligence: Q1 2020 Analytics

McKinsey: COVID-19-19 crisis shifts cybersecurity priorities and budgets July 2020

Interpol report on cyber attacks during covid-19 August 2020

A dual cybersecurity mindset for the next normal

https://assets.kpmg/content/dam/kpmg/au/pdf/2020/covid-19-guide-to-maintaining-business-resilience.pdf

CyberCube: Pandemic under the microscope https://home.kpmg/xx/en/home/insights/2020/04/covid-19-puts-insurers-on-fast-track-to-technology-adoption.html

Tessian: The State of Data Loss Prevention

COVID-19 cyberwar: How to protect your business - https://www.ibm.com/downloads/cas/Y5QGA7VZ

The views expressed in this publication are those of invited contributors and not necessarily those of the IFoA. The IFoA do not endorse any of the views stated, nor any claims or representations made in this publication and accept no responsibility or liability to any person for loss or damage suffered as a consequence of their placing reliance upon any view, claim or representation made in this publication. The information and expressions of opinion contained in this publication are not intended to be a comprehensive study, nor to provide actuarial advice or advice of any nature and should not be treated as a substitute for specific advice concerning individual situations. On no account may any part of this publication be reproduced without the written permission of the IFoA