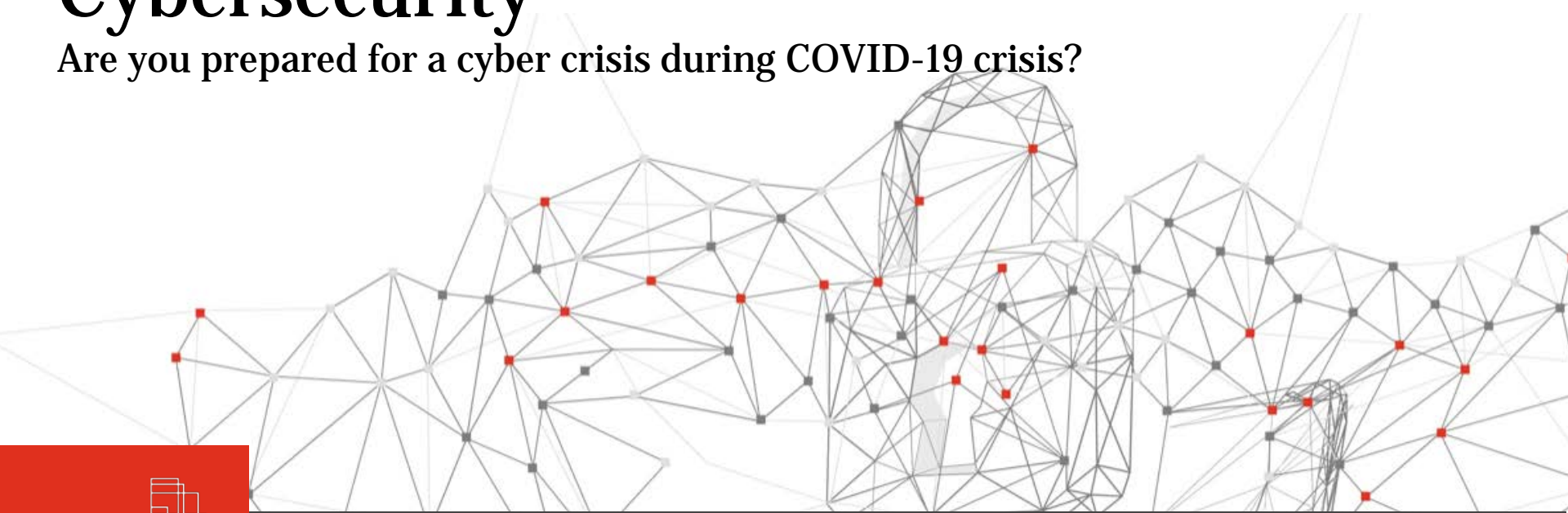


COVID-19

Cybersecurity

Are you prepared for a cyber crisis during COVID-19 crisis?



April 2020

Topics we will cover today

Urs Küderli, Partner Cybersecurity and Privacy

1. Situation

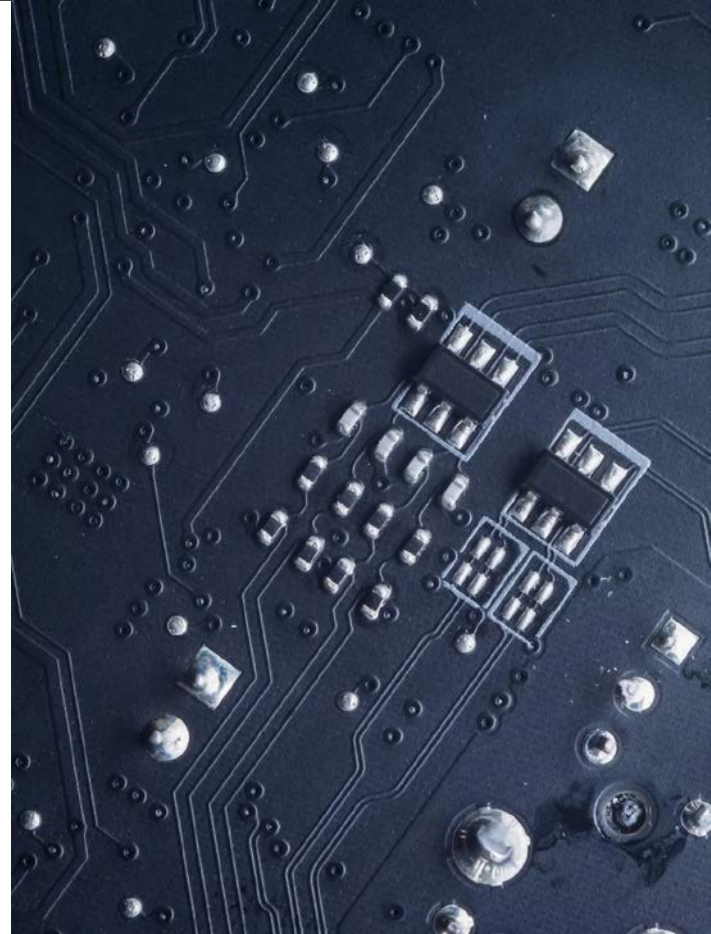
- a. Why Cyber is important in COVID-19 crisis?
- b. Clients in “COVID-19 mode” vs. Cyber Criminals

2. Key topics – what our experts are saying

- a. Emerging COVID-19 threat landscape – Johannes Dohren
- b. Key emerging cyber risks you might face – Yan Borboën
- c. Key priorities to consider - Urs Küderli
- d. Opportunities of change emerging from the crisis - Yan Borboën

3. Q&A – ask your experts now

4. Summary & key take-aways

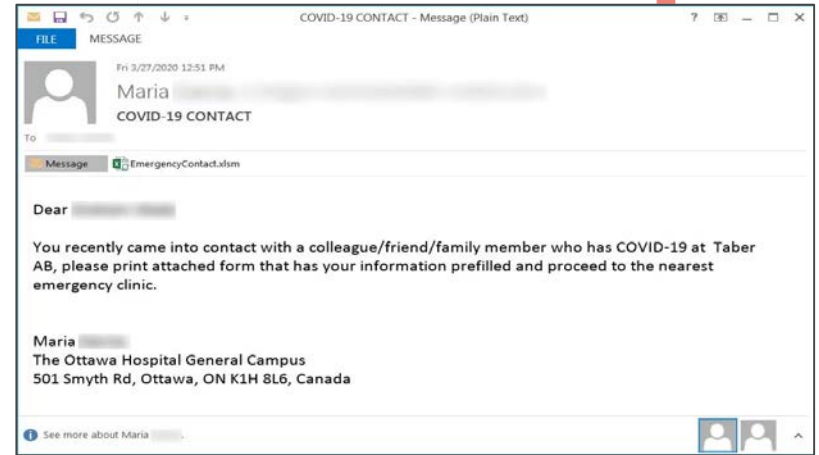


Emerging COVID-19 threat landscape

Johannes Dohren, Director Cybersecurity and Privacy

Attackers View

- Cyber criminals have begun using COVID-19 based phishing campaigns as part of their efforts to infect victims with malware and gain access to their infrastructure.
- Attackers can sit on networks for months and just wait for the right moment to strike.
- In addition to COVID-19-themed phishing campaigns and traditional ransomware, cyber criminals may also begin to take advantage of the changes in the way organisations work.



Phishing example [Source](#)

Example from PwC Threat Intelligence



Some phishing campaigns are using legitimate documents to cover malware downloads



Map from John Hopkins is being used to market a phishing kit and downloader

Key emerging cyber risks you might face

Yan Borboën, Partner Cybersecurity and Privacy

People

Employees might be more vulnerable to social engineering attacks.

Organisations might not be able to respond to cyber attacks due to lack of personnel.

Insider threats may increase.

Process

New vulnerabilities may be introduced.

Existing processes and good practices might be bypassed.

Organisations might be even more vulnerable against cyber attacks.

Technology

Employees are required to work with new technologies.

Technologies tactically and quickly implemented may open new vulnerabilities.

Key priorities to consider

Urs Küderli, Partner Cybersecurity and Privacy

Culture & awareness

End user behaviour and culture awareness during a time of heightened cyber risk



Governance

Operating an effective level of governance in an uncertain environment to maintain an appropriate security posture



Detective controls

Maintaining effective monitoring, detection and protection controls during non-standard business operation



Capacity management

Managing increased demand on the critical security services needed to enable remote working and secure data access



Incident management

Continuing to operate incident management, crisis response and business continuity capabilities during a period of increased organisational stress



Data security

Protecting sensitive information whilst implementing and operating different working practices



What you can do

1. **Invest into your people** - make your employees more aware, more involved and more careful
2. **Detection is key** - understand and monitor your environment, detect internal and external threats fast
3. **Have a “Plan B”** - ensure your crisis and recovery plans work with a remote workforce

What is always true, but more difficult in crisis:

1. **Keep your systems up to date** - decrease vulnerability by keeping your systems up to date, without physical presence

Opportunities of change we see emerging from the crisis

Redefined Meaning of a Resilient Business

Revisit your Disaster recovery and business continuity planning, apply lessons learnt and consider what makes a business resilient.

Accelerated Adoption of Cloud

Companies will reassess how Cloud can help to reduce some of the recent challenges related to remote working and enabling access to key business systems.

Augmented Reality/ Virtual Operations Functions

The use of new technology could change the way businesses and users interact with each other by extending location agnostic services and capabilities and by maximising virtual experiences.



Ask us anything - Q&A



Instructions

In this Q&A, **you** as the audience can get involved, so please submit your questions for the Experts via the **questions box** on your **left hand side**

Summary & key take-aways

What you should keep in mind

1. **Secure** your environment, your people, processes by counter opportunistic threats that take advantage of the situation
2. **Ensure business continuity** by preparing for the worst and have a “Plan B” or response plan
3. **Prepare** to take chances out of the crisis

What you can do: Perform a Cyber risk evaluation

Cyber Attack and Readiness Evaluation (**CARE**), a fully online without any human contact or paperwork assessment tool. This service is tackling the 3 key elements of your cyber defense:

- Cyber risk evaluation: You complete an online questionnaire to evaluate your risks and the maturity of your security controls.
- Technical web security assessment: We perform a vulnerability assessment to understand if you have let doors open to hackers.
- Phishing and awareness campaign for your employees

At the end, you will receive a report describing your main cyber risks, your security maturity level, as well as pragmatic recommendations to help you enhance your security posture and better address cyber-attacks.



Survey: Polling question

Which topic would you like to deep dive into in our next Cyber webinar?

1. Governance - How to operate on effective level
2. Capacity Management - Managing increased demand on critical security services needed
3. Data Security - Protecting sensitive information
4. Cloud business case assessment
5. Remote cyber risks evaluation, employees awareness program, and vulnerabilities assessment
6. Any other topics of interest?

Instructions

At the end of this Webcast, you will see a **box pop-up on your screen**, where you can select one or multiple topics that you would be interested in and click **Submit**



Thank you

One Point of Contact:

Via our crisis helpline and **PwC Switzerland website** ([EN](#) | [DE](#) | [FR](#))

Your experts:



Urs Küderli
Partner
Cybersecurity and Privacy
[Email](#)



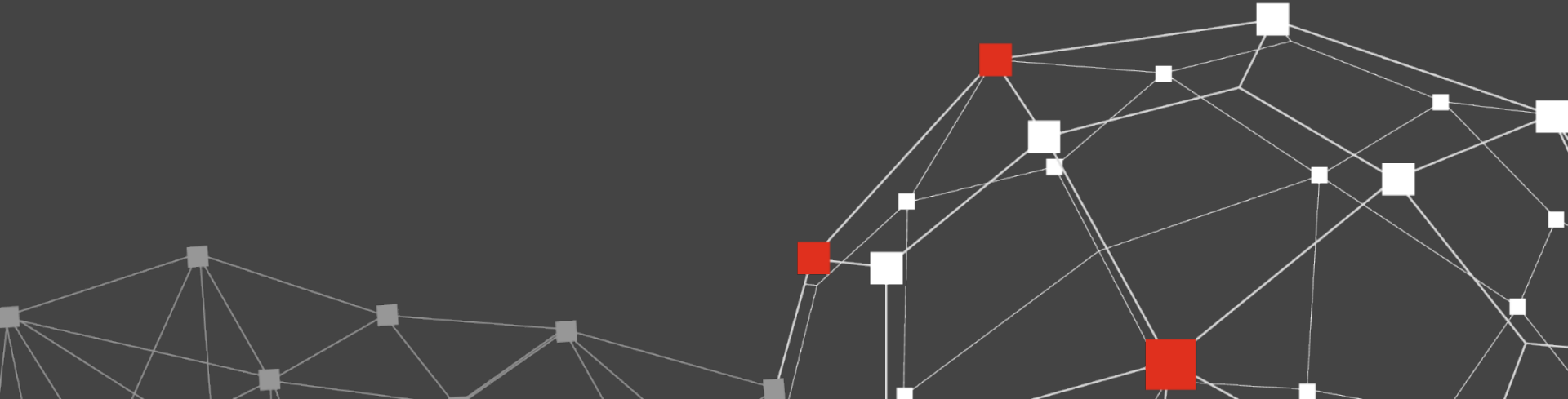
Yan Borboën
Partner
Cybersecurity and Privacy
[Email](#)



Johannes Dohren
Director
Cybersecurity and Privacy
[Email](#)



Additional Material




Securing newly implemented remote working practices


1 Focus Area



Monitor for Shadow IT



Secure Remote Access



Implement Multi Factor Authentication



Review On-premise Security Controls



Enhance Security Monitoring



Adapt Cyber Response

2 Tactical Remediation

Expand endpoint and network monitoring to identify new devices

Monitor spend thresholds and expenses for authorisations of services

Reassess web proxy filtering and consider implementing CASB

Expand VPN capacity (existing capability/ augmented via supplier)

Monitor remote access systems & Active Directory for anomalous logins

Extend/ implement DDOS mitigation

Track / record MFA exceptions

Reconfigure gateways to enable MFA into on premise systems

Switch to cloud applications with native 2FA (where possible)

Tighten data security access & related controls

Review critical security controls/ processes to determine gaps

Establish minimum security operating requirements to maintain consistency

Increase security monitoring capabilities (compensating control)

Move SOC to a high risk footing & implement 24x7 / shift rotation

Augment with third party suppliers to manage load on internal staff

Ensure third-party incident response capabilities are on standby

Focus threat intelligence to identify COVID-19 specific threats (e.g. phishing)

Update processes to reflect contingency and alternative working practices

Ensure the continuity of critical security functions

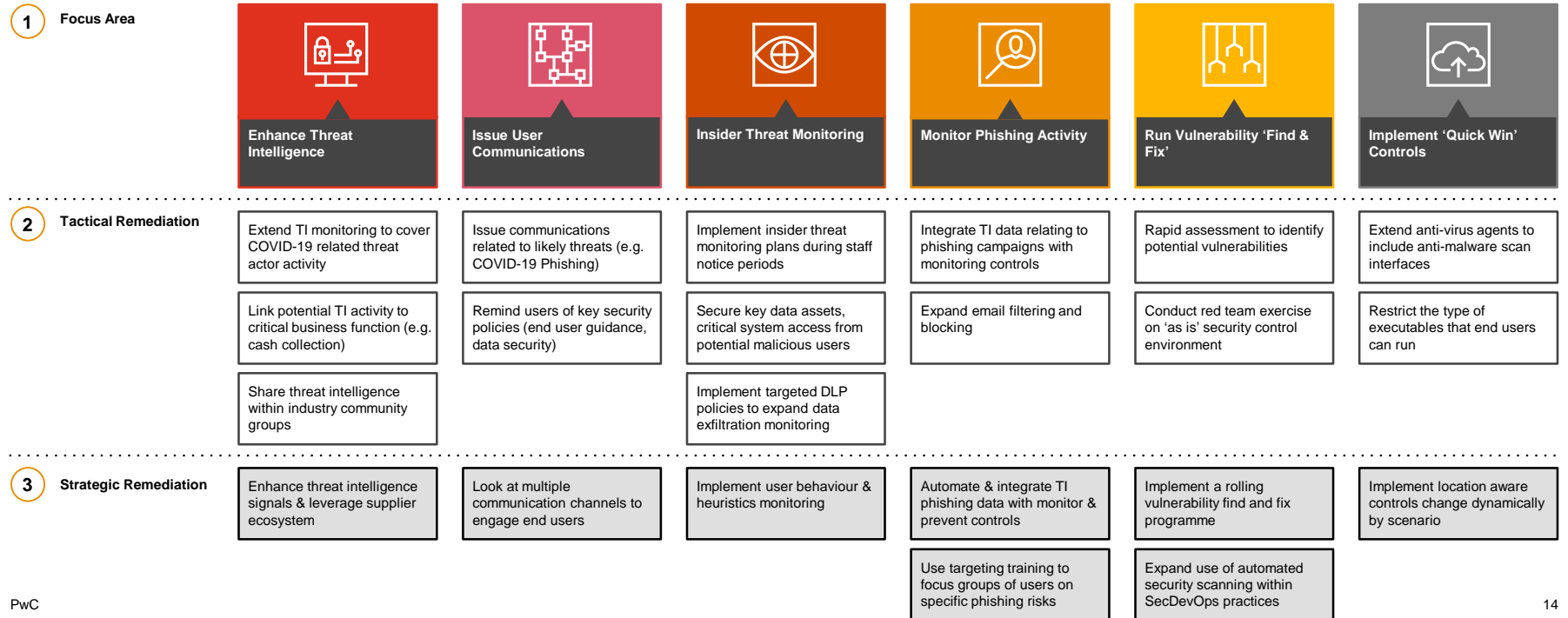
1 Focus Area



2 Tactical Remediation

Assess the impact of recent changes on critical security services	Confirm patching processes are operating for remote connected devices	Assess impact on key security operations (e.g. vuln. mgmt./ patching)	Review backup plans for single points of failure (people/ process/ tech)	Map 'as is' security architecture to identify operational gaps	Track IT assets as they migrate to off-premise locations (physical / logical)
Repurpose IT staff to supplement critical security process	Implement out of band patching for endpoints & critical systems (inc. VPNs)	Implement restrictions on security control changes	Review provisions for enabling remote PAM activity	Document compensating controls where standard sec. arch. is circumvented	Implement asset monitoring for business critical systems & data
Identify business impacts of re-prioritised critical security services	Check BYOD device configurations (e.g. dual homing, AV etc)			Determine quick to deploy cloud security tools as potential interim controls	Restrict access to large repositories of sensitive data

Counter opportunistic threats looking to take advantage of the situation



Thank you!

[pwc.com](https://www.pwc.com)

© 2020 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.