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

Source: Example from PwC Threat Intelligence
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

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

**Focus Area**

1. **Monitor for Shadow IT**
   - Expand endpoint and network monitoring to identify new devices
   - Monitor remote access systems & Active Directory for anomalous logins
   - Reassess web proxy filtering and consider implementing CASB

2. **Secure Remote Access**
   - Expand VPN capacity (existing capability/augmented via supplier)
   - Monitor spend thresholds and expenses for authorisations of services
   - Extend/Implement DDOS mitigation

3. **Implement Multi Factor Authentication**
   - Track/record MFA exceptions
   - Reconfigure gateways to enable MFA into on premise systems
   - Switch to cloud applications with native 2FA (where possible)

4. **Review On-premise Security Controls**
   - Tighten data security access & related controls
   - Review critical security controls/processes to determine gaps
   - Establish minimum security operating requirements to maintain consistency

5. **Enhance Security Monitoring**
   - 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

6. **Adapt Cyber Response**
   - 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

**Tactical Remediation**

- Review On-premise Security Controls
- Enhance Security Monitoring
- Adapt Cyber Response
- Focus Area
Ensure the continuity of critical security functions

1. Focus Area
   - Assess Critical Security Services
   - Enhance Endpoint Security
   - Implement Critical Security Control Change Freezes
   - Review Privileged Access Management
   - Review Security Architecture
   - Monitor Asset Movement

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
   - Implement asset monitoring for business critical systems & data
   - 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
   - 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

PwC
Counter opportunistic threats looking to take advantage of the situation

### Focus Area

<table>
<thead>
<tr>
<th>Focus Area</th>
<th>Tactical Remediation</th>
<th>Strategic Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enhance Threat Intelligence</strong></td>
<td>Extend TI monitoring to cover COVID-19 related threat actor activity</td>
<td>Enhance threat intelligence signals &amp; leverage supplier ecosystem</td>
</tr>
<tr>
<td><strong>Issue User Communications</strong></td>
<td>Issue communications related to likely threats (e.g. COVID-19 Phishing)</td>
<td>Look at multiple communication channels to engage end users</td>
</tr>
<tr>
<td><strong>Insider Threat Monitoring</strong></td>
<td>Implement insider threat monitoring plans during staff notice periods</td>
<td>Implement user behaviour &amp; heuristics monitoring</td>
</tr>
<tr>
<td><strong>Monitor Phishing Activity</strong></td>
<td>Integrate TI data relating to phishing campaigns with monitoring controls</td>
<td>Automate &amp; integrate TI phishing data with monitor &amp; prevent controls</td>
</tr>
<tr>
<td><strong>Run Vulnerability ‘Find &amp; Fix’</strong></td>
<td>Rapid assessment to identify potential vulnerabilities</td>
<td>Implement a rolling vulnerability find and fix programme</td>
</tr>
<tr>
<td><strong>Implement ‘Quick Win’ Controls</strong></td>
<td>Extend anti-virus agents to include anti-malware scan interfaces</td>
<td>Implement location aware controls change dynamically by scenario</td>
</tr>
</tbody>
</table>

- **Link potential TI activity to critical business function (e.g. cash collection)**
- **Remind users of key security policies (end user guidance, data security)**
- **Secure key data assets, critical system access from potential malicious users**
- **Implement targeted DLP policies to expand data exfiltration monitoring**
- **Automate & integrate TI phishing data with monitor & prevent controls**
- **Use targeting training to focus groups of users on specific phishing risks**
- **Expand use of automated security scanning within SecDevOps practices**

---

**Enhance Threat Intelligence**

- Integrate TI data relating to phishing campaigns with monitoring controls
- Rapid assessment to identify potential vulnerabilities
- Extend anti-virus agents to include anti-malware scan interfaces

**Issue User Communications**

- Implement insider threat monitoring plans during staff notice periods
- Expand email filtering and blocking
- Conduct red team exercise on ‘as is’ security control environment

**Insider Threat Monitoring**

- Integrate TI data relating to phishing campaigns with monitoring controls
- Expand email filtering and blocking
- Conduct red team exercise on ‘as is’ security control environment

**Monitor Phishing Activity**

- Rapid assessment to identify potential vulnerabilities
- Extend anti-virus agents to include anti-malware scan interfaces
- Restrict the type of executables that end users can run

**Run Vulnerability ‘Find & Fix’**

- Implement a rolling vulnerability find and fix programme
- Implement location aware controls change dynamically by scenario
- Implement a rolling vulnerability find and fix programme

**Implement ‘Quick Win’ Controls**

- Automate & integrate TI phishing data with monitor & prevent controls
- Use targeting training to focus groups of users on specific phishing risks
- Expand use of automated security scanning within SecDevOps practices

---

**Enhance Threat Intelligence**

- Enhance Threat Intelligence
- Issue User Communications
- Insider Threat Monitoring
- Monitor Phishing Activity
- Run Vulnerability ‘Find & Fix’
- Implement ‘Quick Win’ Controls

---

**Enhance Threat Intelligence**

- Enhance Threat Intelligence
- Issue User Communications
- Insider Threat Monitoring
- Monitor Phishing Activity
- Run Vulnerability ‘Find & Fix’
- Implement ‘Quick Win’ Controls
Thank you!