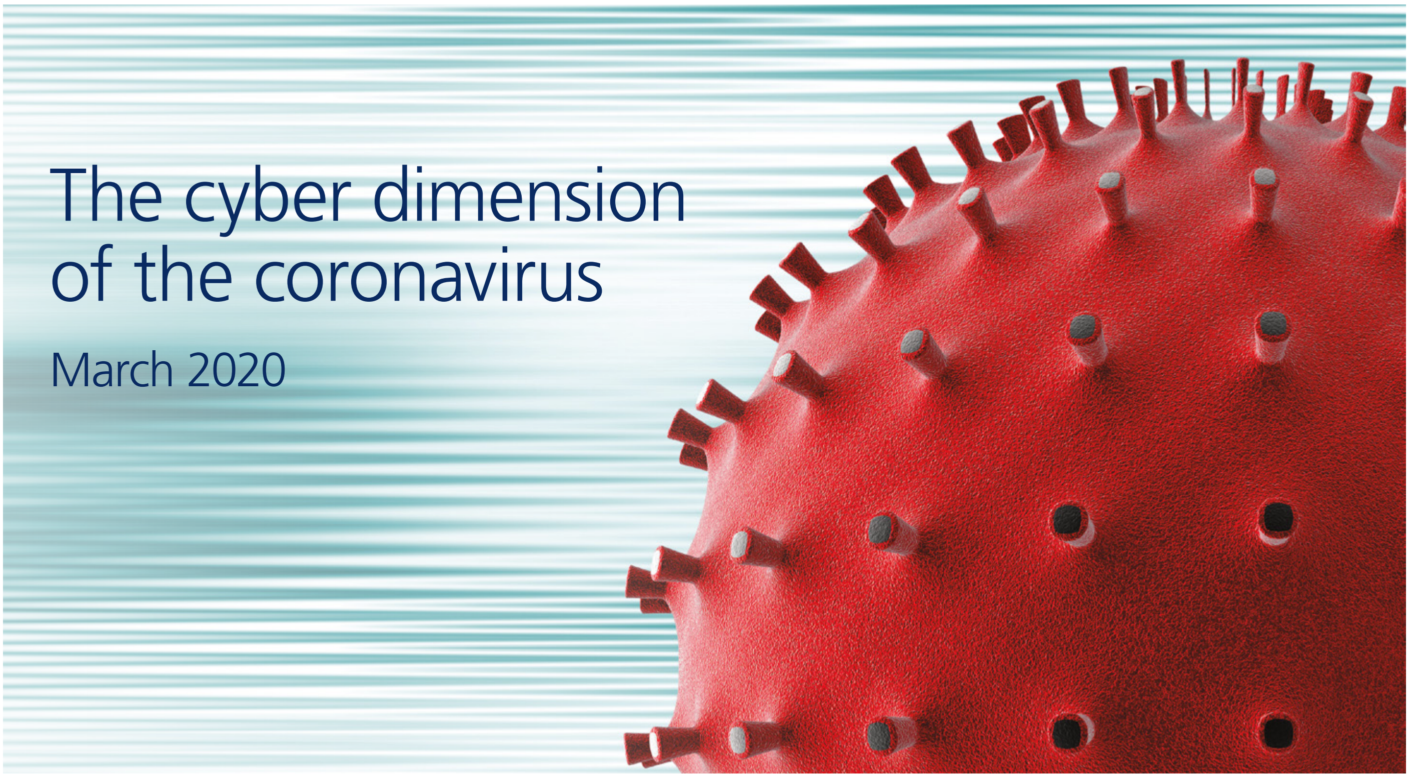
Zurich Commercial Insurance
Risk Insights



The cyber dimension of the coronavirus

March 2020

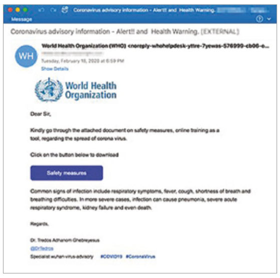
Observations

Over the last few weeks, there has been a dramatic increase in the number of cyber incidents from companies around the world that have been affected by a fresh wave of coronavirus-themed cyberattacks. According to cybersecurity firm CYE, since the beginning of February cybercriminals have been increasingly exploiting the unfamiliar situation caused by the global pandemic. CYE have noted a five-fold increase in cases, particularly across Europe.

By leveraging the public's genuine fear and increased distraction associated with these events, there is an increased likelihood of employees clicking on malicious attachments or using unsecure networks to retrieve sensitive information when working from home or in remote locations. As quarantines become more prevalent and more and more individuals are authorized to work remotely, there must be a multi-departmental focus on maintaining proper controls.

According to recent studies, phishing campaigns and ransomware attacks have seen the greatest increase over the last few weeks, with users clicking on attachments or links delivering a malicious communication using the coronavirus theme.

One sophisticated attack took advantage of the trusted World Health Organisation (WHO), falsely claiming to be from WHO employees asking for sensitive information, to distribute an attachment that stole personal information.



Coronavirus advisory information - Alert!! and Health Warning. [redacted]

Coronavirus advisory information - Alert!! and Health Warning. [EXTERNAL]

World Health Organization (WHO) <noreply-whohelpdesk-yttre-7yewas-576990-cb06-o...
[redacted]
Tuesday, February 18, 2020 at 6:59 PM

Dear Sir,

Kindly go through the attached document on safety measures, online training as a tool, regarding the spread of corona virus.

Click on the button below to download

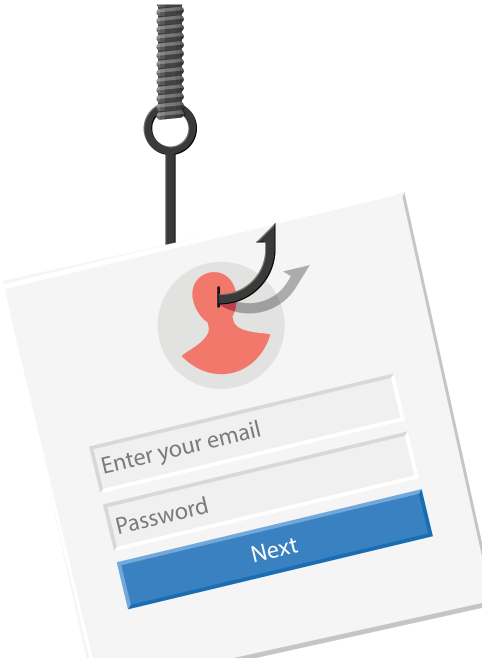
Safety measures

Common signs of infection include respiratory symptoms, fever, cough, shortness of breath and breathing difficulties. In more severe cases, infection can cause pneumonia, severe acute respiratory syndrome, kidney failure and even death.

Regards,

Dr. Tedros Adhanom Ghebreyesus
@DrTedros
Specialist wuhan-virus-advisory #COVID19 #CoronaVirus

Figure 1: screenshot of a phishing email purporting to be from the World Health Organization - source: Proofpoint inc



[1] https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/amp/

Increased cyber risks

Remote and decentralized working increases the risk of falling prey to the following attack types:

Phishing / Spear phishing: Email or other electronic communications with specific information about the recipient embedded to trick the recipient to click on a link, open a malicious attachment or do other compromising actions.

Business Email Compromise (BEC): Email schemes targeting recipients to conduct wire transfers, typically by impersonating the CEO, CFO or other senior managers of the organization.

Social Engineering: Psychological manipulation of people into performing actions they would not normally do.

These events can lead to an increased risk of ransomware that may not only infect and lock the computer networks of businesses and their customers, but also encrypt or destroy data. Recognizing that some forms of cyber attack may lie dormant for days, months, or even years, actions taken today could have a significant impact on a company's earnings and reputation well into the future. Fortunately, there are a number of ways in which both companies and employees can take preventative measures to avoid these activities and maintain a safe and secure digital environment.

Recommendations for risk mitigation

Individuals:

Links/Attachments: Do not click on links or open attachments in emails from untrusted senders. If employees wish to navigate to a website on the internet, it is best practice to directly type the URL of the site they wish to visit. A secure URL will begin with https, instead of http, but this criterion is not enough: Carefully inspect the URL before typing it in to verify it leads to the official website of the company/institution you are trying to access. In case of doubt, use an online URL checker before connecting, such as **isitphishing.org**.

Information: Do not respond or provide account details to unknown sources. Trusted entities such as suppliers or vendors typically already have this information. Never send personally identifiable information and/or passwords via email to unknown individuals or open attachments in unsolicited emails.

Report suspicious activity: All suspicious emails should be reported to the organization's cyber security team, or equivalent department.

Notify the Help Desk: All employees should contact their local help desk if they believe they have opened an attachment or clicked on a link that infected their computer with malware.

Companies:

Employee/User awareness training: Before authorizing remote connections to the corporate network, employees should have adequate training on phishing campaigns and security guidelines, and be knowledgeable about all corporate processes and procedures to report a security incident if a compromise is suspected or identified.

Secure connections: Use only a secured remote access to company networks. Where possible, through a virtual private network (VPN), or another encrypted connection mechanism.

Multi-factor authentication (MFA): VPNs should be configured with multi-factor authentication as an added security layer to ensure that only authorized individuals are accessing the corporate network.

Mobile device management (MDM): Computers, tablets and smartphones of employees should be equipped with a corporate MDM solution. The solution should enforce adequate security controls and create an encrypted virtual environment within the device to store and process corporate information, for instance documents and emails.

Internet perimeter protection: IT departments should ensure that firewalls are properly configured and monitor firewall logging to identify attempted or successful connections from unauthorized or suspicious Internet Protocol (IP) addresses.

Cloud security and compliance: Companies using cloud services should ensure that security configurations are appropriately hardened and monitored for configuration drift or unauthorized manipulation.

Increased monitoring and diligence: If there are geographic regions or countries that employees would have no reason to be remotely connected to on the company network, the IT department should proactively 'blacklist' the IP ranges for those geographies so that they can't remotely connect to corporate networks.

Final thoughts and considerations

It is human nature to focus on the things we see. COVID-19 reminds us that the invisible and the intangible can have a far more damaging impact than some of the more tangible risks we see or read about every day (e.g.: fires, thefts or car accidents). Cyber risks, like COVID-19, fall into this category of intangible risks. Over the last several years, we have seen various events where digital viruses have infected machine after machine and turned into a true pandemic in a short period of time. The NotPetya incident in 2017 was the biggest of these pandemics so far, affecting thousands of companies across the globe, and leading to an estimated economic loss of $10bn. Like today, hygiene is imperative to avoid any infection in the first place. Patching systems and washing hands have equal importance. Sandboxing and quarantines have striking similarities when it comes to managing potential contagion.

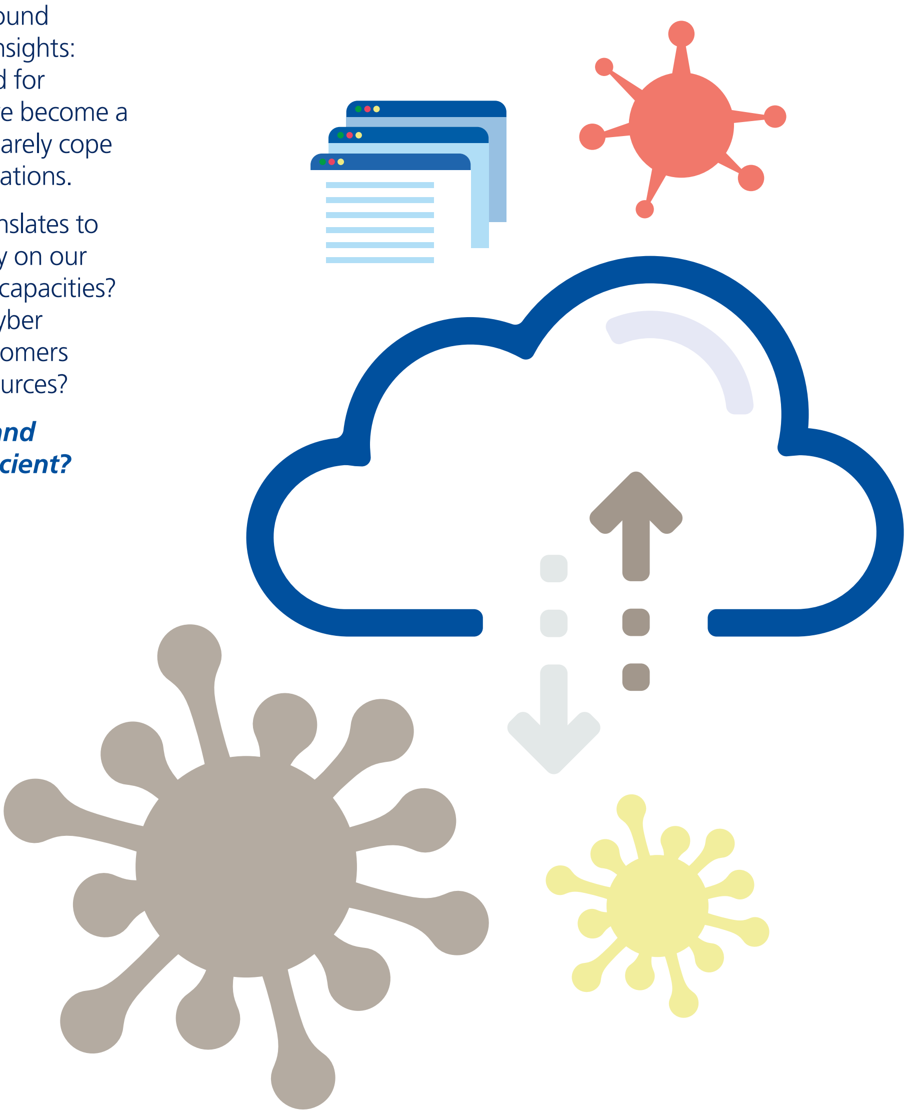
In cyber, the National Institute of Standards and Technology (NIST) provides a framework for companies to foster their capabilities to identify cyber risk, protect, detect, respond and recover from cyber attacks. These capabilities include technology but are not limited to this dimension. As outlined above, awareness and procedures are at the heart of protection. Reliable and fast detection followed by appropriate response and recovery, when needed, is paramount. The current situation around COVID-19 also provides us with the following insights: How do we deal with sudden surges in demand for protection? Hand sanitizers and face masks have become a rare commodity and healthcare providers can barely cope with the increase of patients in intensive care stations.

We should therefore ask ourselves how this translates to cyber and the next cyber pandemic: can we rely on our cyber protection and response capabilities and capacities? Can we rely on external service providers in a cyber pandemic – knowing that they serve many customers and will need to prioritize their own scarce resources?

Are our internal cyber corporate security and emergency response capabilities self-sufficient?

Finally, COVID-19 has shown us the complexity of supply chains and our dependencies on intermediate goods from other countries and continents. Today, this is not only true for physical suppliers but also the suppliers of computing capacity, data storage and platforms on which applications operate.

Over the last several decades, a major trend in manufacturing has been outsourcing, followed by offshoring of services. In information technology, this has been no different. Today, the move into the cloud is the next step, and many companies are currently migrating their IT infrastructures into the clouds of large service providers. The technical opportunity to work far more (cost)efficiently via cloud-based services helps us to respond and to recover from a pandemic real-life event, but it also creates the next intangible, invisible vulnerability. While we are still looking for a 'killswitch' for COVID-19, we can already reflect on what that virus tells us about our digital resilience and cyber security and where we need to prepare for the next cyber virus epidemic.



This document has been prepared by Zurich Insurance Group Ltd and the opinions expressed therein are those of Zurich Insurance Group Ltd as of the date of the release and are subject to change without notice. This document has been produced solely for informational purposes. All information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Group Ltd or any of its subsidiaries (the 'Group') as to their accuracy or completeness. This document is not intended to be legal, underwriting, financial, investment or any other type of professional advice. The Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this document. Certain statements in this document are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by numerous unforeseeable factors. The subject matter of this document is also not tied to any specific insurance product nor will it ensure coverage under any insurance policy. This document may not be distributed or reproduced either in whole, or in part, without prior written permission of Zurich Insurance Group Ltd, Mythenquai 2, 8002 Zurich, Switzerland. Neither Zurich Insurance Group Ltd nor any of its subsidiaries accept liability for any loss arising from the use or distribution of this document. This document does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction.
Zurich Insurance Group

173006686 (03/20) TCL

ZURICH®