

Global Cyber COVID-19 weekly executive cyber briefing

A weekly high-level brief that focuses on some of the most current cyber threats and trends as identified by Deloitte Cyber Threat Intelligence (CTI), with near-term recommendations on managing cyber risks to respond, recover and thrive through the COVID-19 global pandemic.



Managing cyber in the remote workforce

As professionals shift to working remotely from their homes, many are using personal devices versus company-issued machines to access organizational networks and systems. The addition of these devices into an organization's environment is increasing the attack surface and cyber adversaries now have extended access to target and penetrate organizations' most critical assets, data, and operational environments. **The below are a few of the top cyber threats highlighted this week** (and originally identified in our detailed threat report dated March 24 - April 1) impacting organizations globally as they shift to operate with a more distributed workforce.



Cyber risk for virtual communications/teamwork applications

The necessity for millions of professionals globally to continue to meet and work with each other as well as their customers during COVID-19 has spurred the quick adoption of various communication platforms such as Zoom, Microsoft Teams, and Slack.

Observed threat: Home working and learning demands caused quick adoption of the video-conferencing application. Without security controls in place, adversaries may access and join any meetings. In addition, the cloud-based communication platform may allow cybercriminals to access sensitive information such as meeting details and conversations.

Suggested top actions:

1. Ensure discussions over Zoom are not highly sensitive. If so, resort to an alternative platform.
2. Secure all Zoom meetings with passwords at the individual meeting level, or at the user, group, or account level for all meetings and webinars.
3. "Lock meeting" once a meeting begins to prevent additional attendees.
4. Integrate IT and security professionals on expedited tech projects, as well as new technology needs for integration of security controls and general implementation of IT controls.

Impact reach: All industries

Geographies: Global

Prior to the COVID-19 outbreak, **27%** of users globally worked remotely on the average weekday.

As of March 31, 2020

more than

60%

of users work remotely.



Heightened volume of phishing targeted at employees

The economic impacts of COVID-19 have spurred a series of wage subsidies. As employees receive many communications from government entities and their employers, it is critical that they avoid phishing campaigns disguised as relief payment plans.

Observed threat: Recipients of the Coronavirus relief payment from the government opened an attachment from a malicious document used macros to deliver the malware that focuses on obtaining banking information in North America and Europe. We anticipate that this threat will be felt across many geographies as similar government relief plans are put into place.

Suggested top actions:

1. Raise awareness amongst employees who may be receiving a relief payment of malicious phishing campaigns, be specific on what will be shared by your organization (format, timing etc).
2. Bolster threat detection and response to promote proactive identification of malicious activity.
3. Ensure your organization has a crisis response plan and has informed employees to avoid the spread of misinformation.

Impact reach: Government, Public Sector, Banking

Geographies: North America, Europe

Between March 13-26, 2020 there were

over

+400K

incidents of spam emails pertaining to COVID-19



Increased use of personal devices to work remotely

The use of personal devices by employees working from home leads to significant increased risk of cyber adversaries accessing internal infrastructure where data and intellectual property can be accessed. Personal devices may not have the latest security patches and tools or even a VPN connection to ensure a more secure connection to the business environment.

Observed threat: A spam campaign was observed leveraging a fake "Corona Antivirus" lure to distribute malicious software (malware). Using a fake Coronavirus (COVID-19) themed website, threat actors advertised a "Corona Antivirus", which makes bogus claims to protect users from the COVID-19 infection; however, the application infects users with malware.

Suggested top actions:

1. Ensure IT teams develop and implement corporate security policies and guidelines for Bring Your Own Device (BYOD) and require that corporate security software is installed on employee devices before such devices can be used to connect.
2. Review and establish corporate firewall rules for remote access, User Execution and Behavior Analytics (UEBA), file integrity monitoring, to effectively implement for remote employees.
3. Restrict unapproved personal devices from corporate network and only allow personal devices access to corporate cloud services as required for critical business operations.

Impact reach: All industries

Geographies: Global

Without IT's knowledge,

1,000+

insecure personal devices

connect to enterprise networks every day in 30% of the U.S., U.K. and German companies.



Recover and thrive: As COVID-19 continues to evolve at a rapid pace across the globe, organizations will rebound at a varying pace, as they prepare for the “next normal”

For insights on each of the highlighted topics, visit links below.

BUSINESS CONTINUITY & FINANCING

Work and economic climates will continue to contribute to an increased volume of insider threats. Leadership should consider how the enterprise is equipped to pursue a risk-based insider threat monitoring program.

COMMAND CENTER

Security and IT executives should brief senior leadership regularly and ensure there is a clear understanding of leadership’s expectations and their true level of risk acceptance. Threats from early opportunistic attacks remain latent in the environment and pose sustained elevated risk.

CUSTOMER ENGAGEMENT

As markets recover from COVID-19, scrutiny will likely increase in areas of consumer safety, privacy and regulation, influenced by the California Consumer Privacy Act (CCPA), Europe’s General Data Protection Regulation (GDPR), various privacy regulations in South America, and regulatory activities in China, which are improving the cyber posture for organizations and industries across global markets.

DIGITAL CAPABILITIES

Companies should consider balancing their expanding digital footprints with a growing focus on cyber risk. Emerging technologies are often attractive avenues of opportunity for cyber criminals looking to expose weaknesses in an organization’s digital ecosystem. In the absence of a well-orchestrated cyber program, new products and services will be exposed to greater financial, brand, and regulatory risks, likely slowing their development and marketplace penetration.

WORKFORCE & STRATEGY

Many countries still do not have resilient cybersecurity infrastructure, efficient and agile institutions and emergency plans prepared. Investment in more technology, resources and people to strengthen cybersecurity posture will be necessary. With the global understanding of the importance of social distancing – so too can we help train the world to help protect themselves from cyber threats. Changing behaviors through training, awareness, and education is key to the success of any new process. By looking for ways to augment your workforce, organizations can consider managed security services to either operate an existing security program, or onboard to a turnkey solution, organizations may be able to recover faster and with less strain to the broader enterprise.



We’re by your side to help you through COVID-19

Relevant Deloitte reads

- [The heart of resilient leadership: Responding to COVID-19](#) (March 2020)
- [Manage rapid employee return and ramp up future state](#) (March 2020)
- [Design digitally enabled flexible work arrangements](#) (March 2020)
- [Cyber management critical for remote workforces](#) (April 2020)

Deloitte Cyber helps organizations perform better, solving complex problems so they can build confident futures. Smarter, faster, more connected futures—for business, for people, and for the planet. As a recognized leader in cybersecurity consulting, Deloitte Cyber can help better align cyber risk strategy and investments with strategic business priorities, improve threat awareness and visibility, and strengthen our clients’ ability to thrive in the face of cyber incidents. Using human insight, technological innovation and comprehensive cyber solutions, we manage cyber everywhere, so society can go anywhere.

Deloitte China Cyber Risk Partners



Xue, Tony
National Cyber Risk Leader
+86 10 85207315
tonxue@deloitte.com.cn



Jiang, David Wei
Eastern Region
+86 21 23127088
davidjiang@deloitte.com.cn



He, Tommy Xiaoming
Northern Region
+86 10 85125312
the@deloitte.com.cn



Kwok, Eva Yee Ngar
Southern Region, Hong Kong
+852 28526304
evakwok@deloitte.com.hk



Feng, Steven Ye
Eastern Region
+86 21 61411575
stefeng@deloitte.com.cn



Shih, Nathan Pei-en
Eastern Region
+86 21 33138366
nathanshih@deloitte.com.cn



Xiao, Frank Tengfei
Northern Region
+86 10 85125858
frankxiao@deloitte.com.cn



Pihkanen, Miro
Southern Region, Hong Kong
+852 28526778
miropihkanen@deloitte.com.hk



Kukreja, Puneet
Eastern Region
+86 21 33138338
puneetkukreja@deloitte.com.cn



Zhang, Boris Zhen
Eastern Region
+86 21 61411505
zhzhang@deloitte.com.cn



He, Vivi Wei
Southern Region
+86 755 33538697
vhe@deloitte.com.cn



Ma, Luke Kwok Kwan
Southern Region, Hong Kong
+85228521086
lukema@deloitte.com.hk

For more information contact visit [Deloitte.com/covid](https://deloitte.com/covid) or [Deloitte.com/cyber](https://deloitte.com/cyber)

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the “Deloitte Network”) is by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

©2020. For information, contact Deloitte Touche Tohmatsu Certified Public Accountants LLP Beijing Branch.