Building a better working world

EY cyber response to COVID-19

How to strengthen operational resilience and security of financial institutions during and after the COVID-19 crisis

The spread of COVID-19 (coronavirus) could impact more than five million businesses worldwide.[1] In total, the most-affected countries represent nearly 40 percent of the global economy.[2]

Financial institutions and other sectors face an evolving cyber-threat landscape due to impacts from the pandemic.

- Furthermore, a rapid transition to remote work puts pressure on security teams to understand and address a wave of potential security risks.

Recent cyber threats and attacks

- **Phishing, malicious sites, and business email compromise**
  - Cyber criminals are exploiting interest in the global epidemic to spread malicious activity through several spam campaigns relating to the outbreak of the virus.
- **Extortion or information theft and brand damage**
  - May target organizations perceived as under pandemic-related pressure.
  - Actions or statements considered inappropriate could trigger "hacktivism" and insider threats.
- **Business disruption from attacks**
  - "Coronavirus-themed ransomware", which can encrypt a computer's hard drive and let hackers demand payment to unlock it, has also been used.
- **Dispersal of previously in-person activities and processes**
  - Change in network baseline:
    - Remotely performed high-privilege actions could trigger alarms.
    - All traffic will appear anomalous until new baseline is established.
  - Increased load on help desk and IT.

"

79% Board members state that their organizations are not very well prepared to deal with a crisis event.[3]

- European Central Bank sent a letter to significant institutions to remind relevant issues in order to control and contain potential pandemic risk in their contingency strategies.
  ECB Letter
- Coronavirus-themed domains 50% more likely to be malicious than other domains.
  CheckPoint
- Thousands of COVID-19 scam and malware sites are being created on a daily basis.
  ZDNet
- Coronavirus Scam Alert: Watch Out For These Risky COVID-19 Websites And Emails.
  Forbes
- Attacks pretend to be from the Center for Public Health of the Ministry of Health of Ukraine and deliver bait document.
  RedDrip Team

[1]Source: CNBC, 4 February; [2]Source: McKinsey, [3]Source: Global Risk Survey 2020

The following actions could be considered to help protect your organization during this rapidly changing environment and recent cyber-threats landscape.

- Define and refine manual supporting remote and secure access to corporate environment.
  Ensure IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications such as rate limiting – to prioritize users that will require higher bandwidths.
- Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations and activation of internal and peripheral security functions.
- Implement multi-factor authentication (MFA) on all VPN connections to increase security. If MFA is not implemented, require teleworkers to use strong passwords.
- Limit administrator access and activities to the strictly necessary. Admin activities should also be better monitored and controlled (for example with a four-eyes principle).
- Closely monitor privileged access by optimizing the behavioral analytics tools for detecting suspicious activity for admins and those who handle critical data.
- Support to enable or to verify (in terms of capabilities and security functionalities) collaboration tools (Microsoft Teams/ Skype, Cisco Webex).
- Security information and event management (SIEM) systems should be adapted, strengthening the log-monitoring rules to trigger an alert. Security operation center (SOC) and monitoring teams should be available to manage the increased number of alerts, sorting them by risk, based on a strong process and detecting false-positives from real suspicious events.
  For that, set up event triage/analysis team and consider staff increase.
- Prepare for the worst, check crisis management and incident response capabilities internally and also availability of your third parties, maybe extend your provider landscape.
- Pay better attention on the following remote access cybersecurity tasks: log review, attack detection, and incident response and recovery.
- Increase your endpoint monitoring protection.
- Increase emergency management capacities, by reallocating resources. Check if your backup is working, test your failover capabilities. Help Desk should also be prepared to handle an increased number of events and the procedure to categorize those events.
- Enhance monitoring and detection capabilities to identify malware or campaigns that are leveraging the present scenario implementing whitelisting and marking external emails to inform employees about an expected increase in phishing attempts with corona-related topics and ask to don't click unknown suspicious links.
- Web and email protection by implementing web-filtering technologies to prevent employees from visiting malicious websites. Implement email-filtering rules to block spam and phishing emails. If you are a hospital or have a critical structure, you need to be stricter and consider whitelisting.
- Take action to reduce the impact of fraud attempts on payment systems related to the COVID-19 outbreak. Numerous coronavirus-related websites and emails are being used for phishing campaigns to steal credentials and spread malware.

What messages should be passed to your employees

1. **Consistently follow your company policies**
   Policy, guidelines and rules for accessing the company network outside the office. Make sure to report any suspicious behavior to support and follow basic standards. For example: keep up-to-date operating systems, antivirus and malware, regular scanning, etc.
2. **Don't allow family members to use your work devices**
   Treat your laptop, mobile device and sensitive data as if you were in your office location.
3. **Use your company-approved storage solution**
   Make sure to store all your work data in a secure location that is approved by and accessible to your company.
4. **Only use company-approved devices and consult your IT department if you will be using a personal device to connect to corporate networks**
   If connecting through your home Wi-Fi, ensure that it has a strong password and avoid using public or unsecured networks.
   If a personal device must be used, on an exception basis, be even more careful updating operating systems, antivirus, update FritzBox Router, etc.
5. **Be mindful of your online hygiene**
   Be careful of clicking on suspicious links, especially if related to coronavirus, as attackers are using that fear to click without thinking.

Your EY Team

UK

Steve Holt
sholt2@uk.ey.com

Ali Kazmi
akazmi@uk.ey.com

Jack Armstrong
jack.armstrong@uk.ey.com

Germany

Lars Weimer
lars.weimer@de.ey.com

Dr. Christoph Capellaro
christoph.capellaro@de.ey.com

Italy

Fabio Colombo
fabio.colombo@it.ey.com

Donatella Laudati
donatella.laudati@it.ey.com

Switzerland

Tom Schmidt
tom.schmidt@ch.ey.com

Reto Aeberhardt
reto.aeberhardt@ch.ey.com

Nordics

Claus Thaudahl Hansen
claus.t.hansen@dk.ey.com

Netherlands

Tony de Bos
tony.de.bos@nl.ey.com

Ireland

Howard Shortt
howard.shortt@ie.ey.com

France

Imad Abounasr
imad.abounasr@fr.ey.com

Spain

Julio San Jose Sanchez
julio.sanjosesanchez@es.ey.com

Luxembourg

Thomas Koch
thomas.koch@lu.ey.com

Portugal

Sergio Martins
sergio.martins@pt.ey.com

Belgium

Ben Van Erck
ben.van.erck@be.ey.com