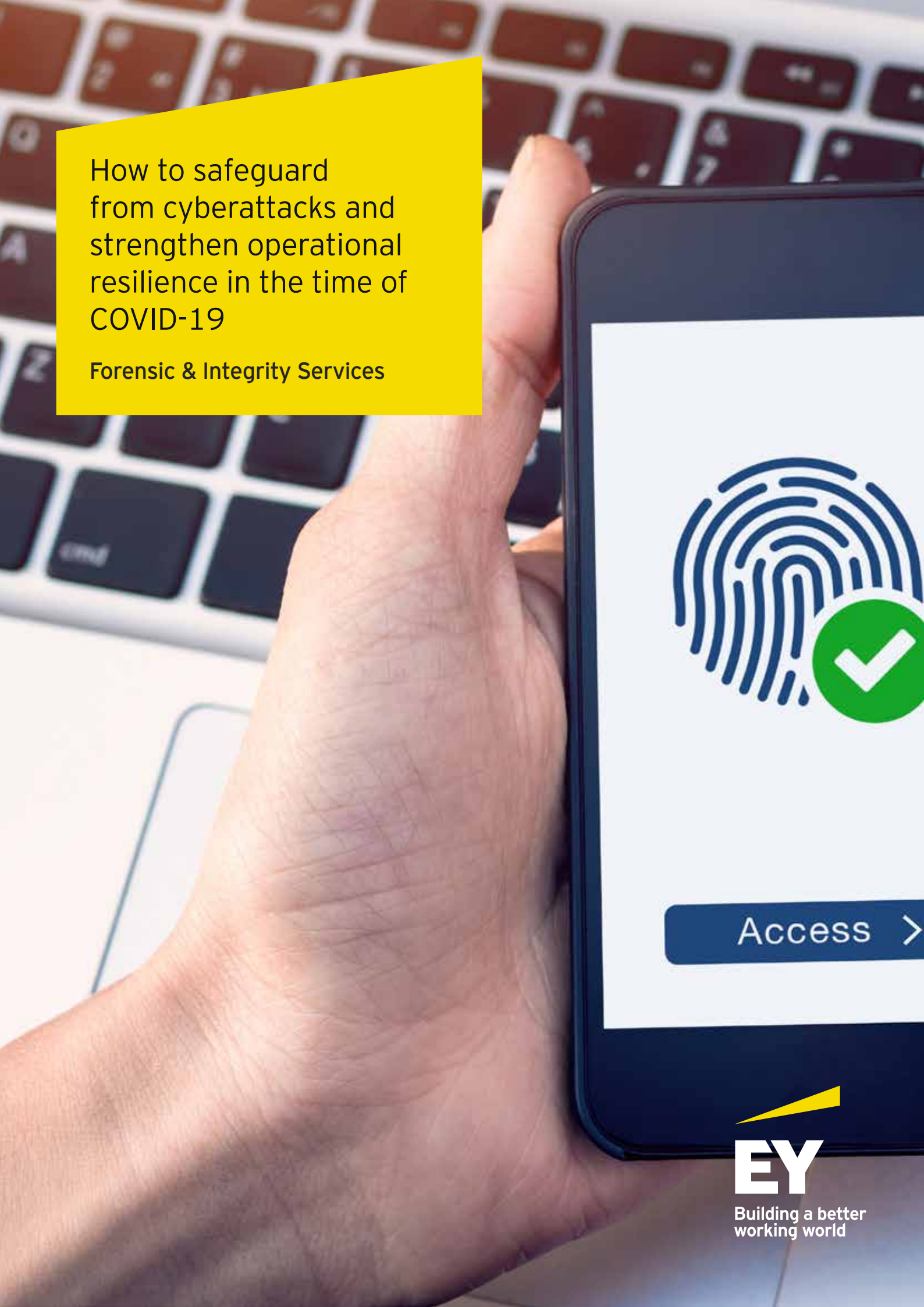
How to safeguard from cyberattacks and strengthen operational resilience in the time of COVID-19

Forensic & Integrity Services



EY
Building a better working world

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

40%

of the global economy.[2]

Organizations face an evolving cyber threat landscape due to the pandemic's impact

A rapid transition to remote working puts pressure on security teams to understand and address a wave of potential security risks.

79%

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

Recent cyber threats and attacks

Phishing, malicious sites and business email compromise

Cyber criminals are exploiting the public interest in the global epidemic to carry out malicious activities through several spam campaigns related to the outbreak of the virus

Extortion or information theft and brand damage

Organizations perceived as being under pandemic-related pressure may be targeted

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 helpdesks and IT

> 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**

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

The following action could be considered to protect organizations in this rapidly changing environment with a dynamic cyber-threats landscape.

01 Define and refine manual **supporting remote and secure access to corporate environment**

02 Have 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

03 **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

04 Implement **multi-factor authentication (MFA)** on all VPN connections to increase security. If MFA is not implemented, require teleworkers to use strong passwords

05 **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)

06 Closely **monitor privileged access** by optimizing the behavioral analytics tools for detecting suspicious activity for admins and those who handle critical data

07 Support enabling or verifying (in terms of capabilities and security functionalities) **collaboration tools** (Microsoft Teams, Skype, Cisco Webex)

08 **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**

09 Prepare for contingencies, **check crisis management and incident response capabilities** internally and also availability of your **third parties,** maybe extend the provider landscape

10 Pay better attention on the following **remote access cybersecurity tasks:** log review, threat hunting, attack detection and incident response and recovery

11 Increase **endpoint** monitoring protection using strong DLP tools

12 Increase **emergency management capacities,** by reallocating resources. Check if the backup is working, **test failover capabilities.** A helpdesk should be prepared to handle an increased number of events and the procedure to categorize those events

13 Enhance monitoring and detection capabilities to **identify malware or campaigns** that are leveraging the present scenario by implementing whitelisting and marking external emails to inform employees about an expected increase in **phishing attempts** with corona-related topics. Don't click unknown or suspicious links

14 **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. In case of a hospital or those with a critical structure, be stricter and consider whitelisting

15 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 employees

1

Consistently follow company policies, including all do's and don'ts

- Report any suspicious behavior to support and follow basic standards. For example: keep operating systems updated, set up antivirus and anti-malware software and conduct regular scanning

2

Restrict the usage of work devices and avoid allowing family members to use them

- Treat the laptop, mobile device and sensitive data as if being in the office

3

Use company-approved storage solution through secured VPN gateways

- Store all work data in a secure location that is approved by and accessible to the company

4

Only use company-approved devices and consult the IT team if using a personal device to connect to corporate networks

- If connecting through home Wi-Fi, create 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

5

Be mindful of online hygiene

- Do not install any new or unwanted software's without the permission of the company's IT team
- Always double check emails received from external vendors or third parties, so they are coming from known sources. Do not click on any links or open any attachments in the email without having anti-virus software in the laptop

For more, contact us

Arpinder Singh
Partner and Head India and Emerging Markets
Forensic & Integrity Services
P: + 91 12 4443 0330
E: arpinder.singh@in.ey.com

Harshavardhan Godugula
Partner
Forensic & Integrity Services
P: +91 98 6666 0790
E: harshavardhan.g@in.ey.com

Ranjeeth Bellary
Associate Partner
Forensic & Integrity Services
P: +91 98 6632 1644
E: ranjeeth.bellary@in.ey.com

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY Forensic & Integrity Services

Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

EYIN2004-034
ED None

ey.com/in

@EY_India EY YouTube EY India

EY Careers India ey_indiacareers