Capgemini RESEARCH INSTITUTE

APRIL 2020

# Boosting cybersecurity immunity: Confronting cybersecurity risks in today's work-from-home world

As the COVID-19 pandemic tightens its grip, working from home becomes the new normal for numerous organizations. According to a recent survey, 85% of companies say at least half of their workforces are working from home due to COVID-19.[1]

The shift to a work-from-home operating model raises significant implications for IT and cybersecurity, with risk on the rise. For instance, at Cisco Systems, the number of requests for security support for remote workforces jumped ten-fold in the last few weeks.[2] There are also heightened risks of state-sponsored attacks to penetrate critical infrastructure such as healthcare, relief agencies, and financial services.[3] Critical infrastructure, including hospitals and food delivery services, have seen increased attacks. A healthcare facility in Europe was recently hit by a cyberattack severe enough to require urgent surgery be postponed, critical patients transferred to nearby facilities, and the entire IT network shut down.[4]

During this crisis, two factors are important for business leaders. First, understanding why cybersecurity must be a key focus area for their organizations during the COVID-19 crisis. And second, understanding what best practices are critical for improving security for remote employees.

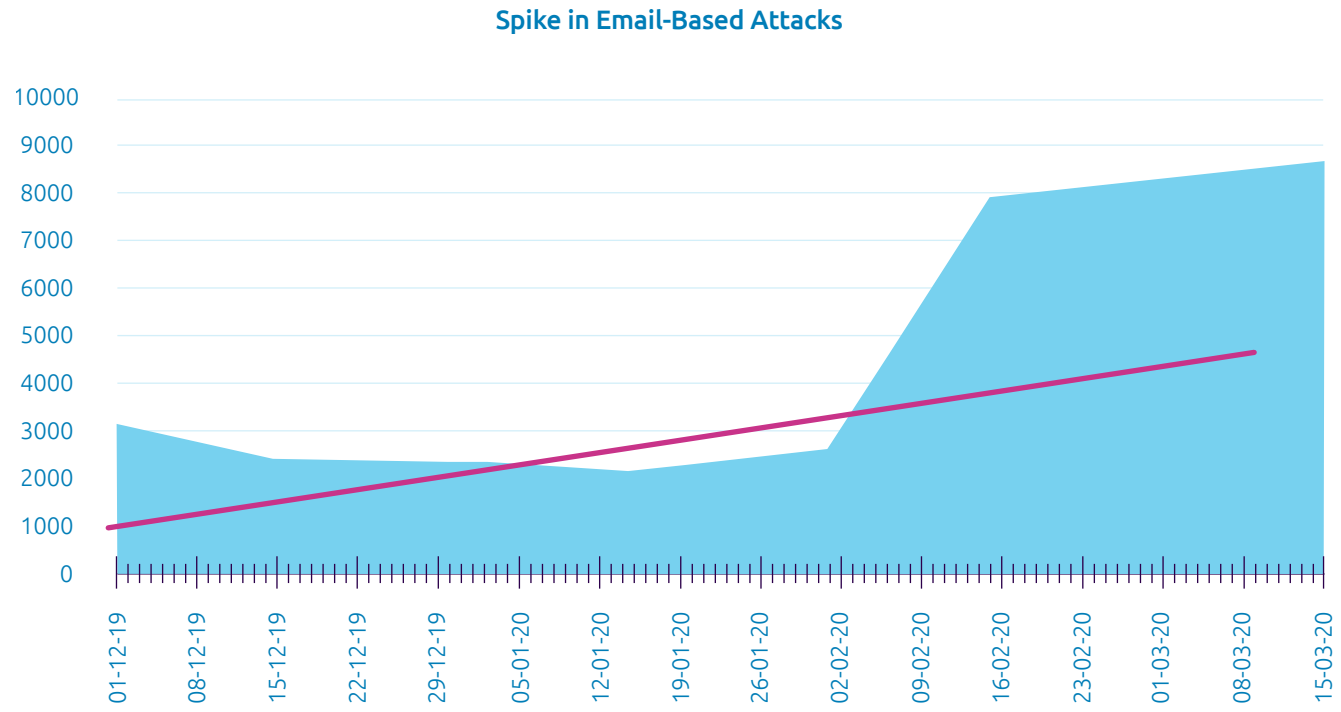
## Cybersecurity needs to be front and center during the COVID-19 crisis

The COVID-19 crisis brings multiple cybersecurity challenges. A situation where employees are commonly working from home provides more opportunities for hackers – a result of the change in the attack surface and work environment. Hackers are also enticing employees and the public to access fraudulent websites and open phishing emails, preying on the fact that people are anxious for advice, guidance and news on the coronavirus. These cybersecurity attacks exploit the fear and doubt that the coronavirus has created in minds, enticing people into making poor security decisions. For example, hackers mount cyberattacks by asking employees to download the latest data on coronavirus from a website, or provide their organization's details for government grants.

Tom Hale, SurveyMonkey president confirms this trend, saying: *"We've definitely seen an uptick in COVID-19 phishing attempts that are making emotional appeals and using the crisis to drive urgency."* [5]

In Italy, one of the countries worst affected by the virus, the first wave of the pandemic saw a spike in anomalous email logins (see Figure 1).

**Figure 1:** Italy sees spike in cybersecurity incidents




**Source: Cynet global threat telemetry data, March 2020** [6]

We are seeing a similar phenomenon in other countries recently. The French cybersecurity agency published a warning on ransomware attacks targeting local authorities.[7] Spear-phishing emails (personalized emails sent to targeted users to trick them into sharing sensitive information) also increased at a tremendous pace over the last three months. For instance, spear-phishing email attacks related to COVID-19 have increased by 667% since the end of February.[8] *"I've never seen this volume of phishing. I am literally seeing phishing messages in every language known to man,"* adds Marc Rogers, VP of cybersecurity strategy at Okta, an identity and access management company and Defcon's head of security.[9]

## Enhancing the security of remote employees

While the world deals with a massive humanitarian crisis with COVID-19, organizations also need to urgently address the heightened cybersecurity risks that come with this situation. In our experience, best practice response involves three distinct phases:

**667%**

INCREASE IN SPEAR-PHISHING EMAIL ATTACKS RELATED TO COVID-19 SINCE END OF FEBRUARY

**PHASE 1**

- Educate employees on COVID-19 cybersecurity issues
- Develop cybersecurity guidelines for employees working from home

**PHASE 2**

- Improve remote surveillance and capabilities to detect cyber threat
- Augment cybersecurity capabilities with AI-enabled tools
- Deploy security orchestration, automation and response
- Collaborate externally to share COVID-19 related cyberattacks

**PHASE 3**

- Plan for a staggered return to the corporate network
- Identify potential failure points in the systems and revamp security protocols

### Phase 1: Educate employees on COVID-19 cybersecurity challenges

Comprehensive cybersecurity guidelines need to be developed for employees working from home and updated and shared in real time. Matt Petrosky, vice president of customer experience, GreatHorn, a cloud-native email security company says, *"Organizations should...build mechanisms to reinforce such policies in the moment they most need be followed – for example within the context of an email asking for financial action or confidential information – so that users can make informed decisions before interacting with suspicious emails. By providing employees with reminders about policies when it matters, companies can significantly reduce risk for their remote workforce."* [10]

Other key elements of education include:

- Run security awareness campaigns across the organization to educate employees on the cybersecurity challenges they may face as they work from home.
- As employees work from home, they may not be able to access internal communications channels via secure VPNs and internal company webpages may not be the right way to educate employees. Establishing alternate communication channels for communication that do not require a VPN is critical to ensuring that all employees receive regular cybersecurity updates.
- Inform employees about email-based fraud and malware schemes that take advantage of the pandemic. Examples include fake emails claiming to be from authentic sources

such as the Center for Disease Control and Prevention (CDC), the World Health Organization (WHO), government sources or health insurance firms. Office emails should be a vital source of information for employees and educating employees on email-based security issues will be important.

- Ensure employees are vigilant about emails that want them to share personal data with regard to receiving government grants to purchasing cures, vaccines, and testing kits.
- Inform employees about the potential risks of using non-approved storage systems, including the threat of data theft.
- Educate employees on the risks associated with data leaks or breaches of personal data confidentiality as enshrined in legislation like the GDPR, as employees may be using personal devices that may be shared by other members of their family.
- Share a list of approved third-party collaboration tools for employees – some collaboration tools may have security flaws employees may not know about.

### Phase 2: Improve remote surveillance and detection of cyber threats

While many remote employees will be using company-issued devices – such as laptops – the use of personal devices will also be prevalent. With increased use of personal devices, a number of steps are critical:

- Ensuring that applications that hold sensitive data are accessed through a remote desktop application.
- Ensuring company-issued devices can be remotely wiped clean in the event of a breach.
- Putting in place continuous monitoring of any devices that are used to access and share confidential data

US-based First Horizon Bank previously had about 30% of the staff with work-from-home capability, but with COVID-19, this has now increased to 50%. The bank already had a VPN system but it is now adding various tools – such as virtual desktops – to expand work-from-home options. The bank has also tackled cybersecurity head-on by adding multiple protection mechanisms and closely monitoring their networks. *". . . as we've moved more and more people to this remote work model, [we have been] trying to make sure that we maintain our controlled environment,"* Bruce Livesay, CIO of First Horizon, said. *"There's no doubt hackers are out there looking for ways to take advantage of this."* [12]

Augmenting Identity and Access Management (IAM) is critical as hackers with stolen credentials will attempt to access important data. For highly regulated sectors, such as financial services and healthcare, this will be an important area to consider during this crisis. Ensuring multi-factor authentication and reviewing single sign-on for critical applications will help improve the security. For instance, software organization 'Autodesk' is expanding the use of two-factor authentication, monitoring risks in the company's technology supply chain during the pandemic crisis.[13]

### *Augment cybersecurity analysts' capabilities with AI-enabled cybersecurity tools*

Security analysts have a huge task ahead of them. With employees logging in from multiple devices over the past few weeks, segregating genuine threat alerts from false positives will be challenging. But even before COVID-19, 56% of organizations said their network security analysts were "overwhelmed" – a result of the vast array of data points and end-point devices they had to track.[14] In this resource-constrained environment, agility will therefore be key. At Siemens, the use of AI has enabled the organization to increase security without a massive increase in resources. The

> "WE'VE DEFINITELY SEEN AN UPTICK IN COVID-19 PHISHING ATTEMPTS THAT ARE MAKING EMOTIONAL APPEALS AND USING THE CRISIS TO DRIVE URGENCY."
>
> **Tom Hale,**
> President, SurveyMonkey

Siemens Cyber Defense Center (CDC) used AWS (Amazon Web Services) to build an AI-enabled, high-speed, fully automated, and highly scalable platform to evaluate 60,000 potentially critical threats per second. AI allowed them to deliver this capability with a team of less than a dozen people.[15] Our research found that with AI, the overall time taken to detect threats and breaches is reduced by up to 12%.[16]

### *Deploy security orchestration, automation and response to improve security management*

Security orchestration, automation, and response (SOAR)[17] are technologies that enable organizations to collect security data and alerts from different sources, leveraging human and machine power for incident analysis. This helps define, prioritize and drive standardized incident response activities with improved metrics and reporting and lower time to respond. However, our research found that only 36% of firms have deployed it to date.[18]

### *Collaborate externally to share COVID-19 related cyberattacks*

Platforms to collaborate with other organizations and share the latest threat data are always important, but particularly so in today's virtual working environment:

- Europe's large financial organizations (including Mastercard Europe, Banque de France, SWIFT, De Nederlandsche Bank, Euroclear) joined forces with the European Central Bank to share intelligence on cybersecurity threats through the Cyber Information and Intelligence Sharing Initiative (CIISI-EU).The information will be shared through an online exchange and will help them counter emerging cyber threats effectively.[19]
- IBM's X-Force, a proprietary platform for shared threat intelligence, discovered the Emotet attack. This was malware that emerged to exploit the COVID-19 situation in Japan, using a phishing email that purported to be from a disability welfare provider. When the document contained in the email was opened, it downloaded and installed Emotet.[20]

**12%**

OVERALL REDUCTION IN TIME TAKEN TO DETECT THREATS AND BREACHES WITH AI

However, despite the clear benefits of this approach, many organizations are not working together. According to research we conducted into AI in cybersecurity, only one in two executives say they share threat intelligence outside their organization through crowdsourcing platforms.[21]

Today, organizations are creating communities focused on COVID-19 related cyberattacks. Yousuf Khan, CIO of Automation Anywhere, a robotic process automation software firm, says, *"We're ensuring open lines of communication with employees, partners and customers to identify and resolve issues in real-time. A crisis such as COVID-19 can bring a global community together, and technology can be an important conduit to solve immense problems."*[22] Another community is the COVID-19 CTI (cyber-threat intelligence) League, with more than 800 cybersecurity experts across 40 countries. This community is managed by tech execs from Microsoft, Okta, Amazon and Clearsky Cyber Security and and it prioritizes the defense of front-line medical resources and critical infrastructure.[23]

## Phase 3: Plan for a staggered return to the corporate network

While security controls may work efficiently in the company corporate network, they are not necessarily as efficient for work-from-home environment. For instance, a VPN might not be able to sustain the high traffic generated when so many employees are working from home. And, with employees working for extended periods without connecting to the company's VPN, their laptops or desktops may be behind with regular updates and patches. *"Since many of the security controls and tools used by non-distributed companies depend on being on the local network, they cannot do [many] things remotely,"* Lisa Davies, head of corporate security at Redox, a healthcare technology firm said. "*These companies have found it more difficult to update, monitor logs etc unless the device is on the local network, so when employees take them home, they are in the dark."*[24]

Once the situation returns to normal, there is a chance that employees' laptops might have been compromised during the crisis. Ensuring that the latest anti-virus patches are updated, and devices are screened in a staggered manner before being connected to the company network, will be essential.

Every crisis, however grim, opens a window to new learning. This is especially true for organizations that did not have tried-and-tested work-from-home arrangements in place. Cybersecurity capabilities will be stress-tested because of the surge in remote application volumes. By monitoring this closely, and identifying glitches in cybersecurity practices, organizations can identify failure points in their systems and revamp security protocols, such as data access and transfer.

Wayne Sadin, chief digital officer at marketing services company, Affinitas Life, says: "*Even if you don't have everything in place for a fully functioning, work-from-home plan right now, it is a good time to test what you do have and make optimizations."*[25]

## Conclusion

COVID-19 has stress-tested society and the global economy to a significant degree, from the integrity of our health systems to the efficacy of global supply chains. It is also stress-testing our cybersecurity defenses. However, the investment and focus that companies bring to the issue now will allow them to emerge even stronger in the future – armed to exploit new technology advances and operate in a world where working from home will become increasingly a fact of life.

*This document is part of the Capgemini Research Institute's special series of research notes on pragmatic tips to help organizations tide over the COVID-19 pandemic. You can find more such research notes and other tips and analyses at* ***https://www.capgemini.com/our-company/covid-19-insights-for-today-and-tomorrow/***

## Authors

**Thierry Daumas,** Head of Projects & Consulting, CIS and Global Offer Lead (GOL), Cybersecurity; **Steve Wanklin**, Capgemini, Group Chief Cybersecurity Officer; **Geert van der Linden**, Cybersecurity Business Lead; **Sandeep Kumar**, Vice President, Capgemini Invent, UK; **Jerome Buvat**, Global Head of Research and Head of Capgemini Research Institute; **Subrahmanyam KVJ**, Director, Capgemini Research Institute; **Sumit Cherian**, Manager, Capgemini Research Institute; **Gaurav Aggarwal**, Manager, Capgemini Research Institute and **Shahul Nath**, Consultant, Capgemini Research Institute have contributed to this research note.

## For more information do reach out to us:

**Global**

**Thierry Daumas**
Head of Projects & Consulting, CIS and Global Offer Lead (GOL), Cybersecurity
thierry.daumas@capgemini.com

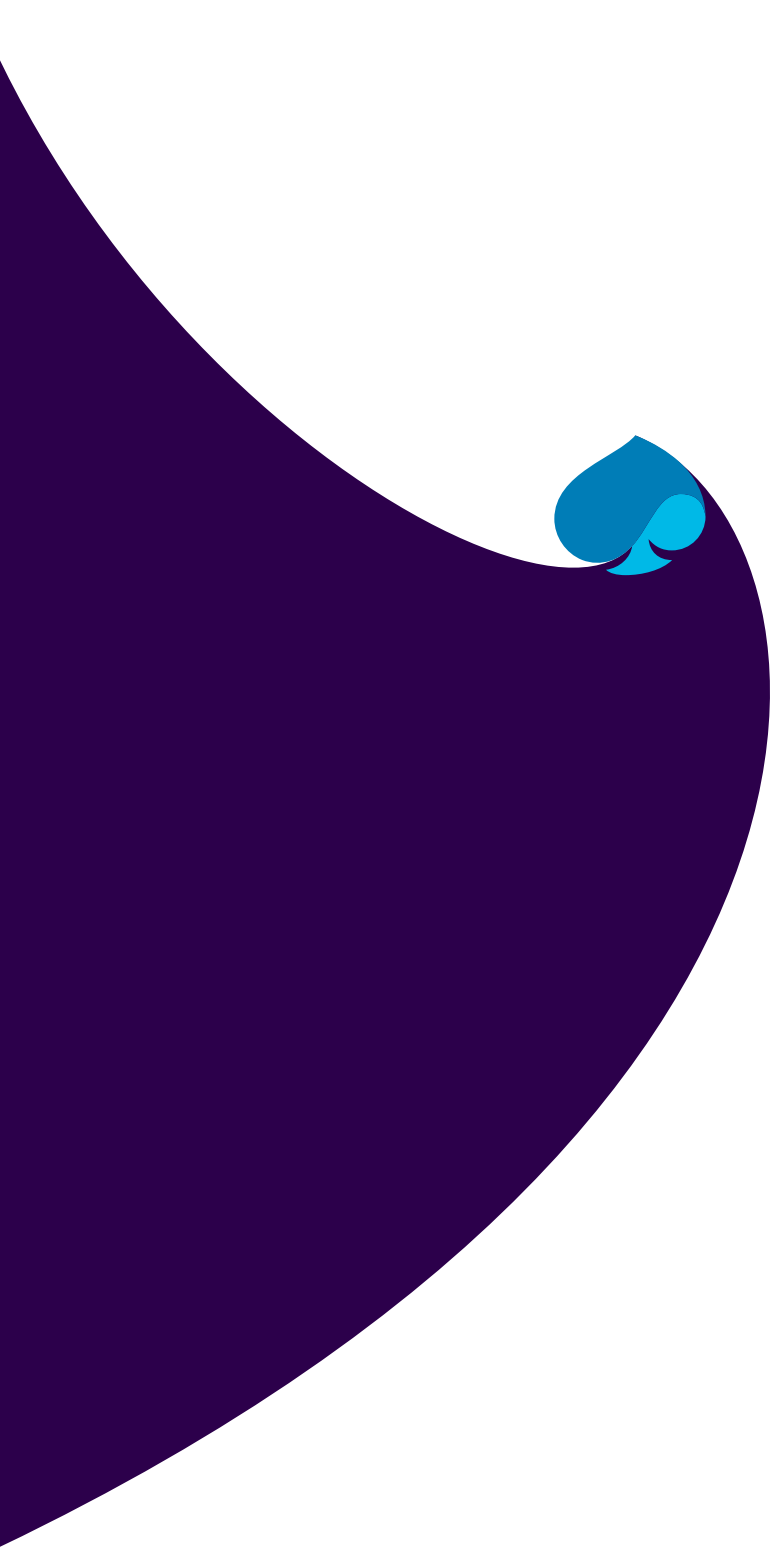
**Geert van der Linden**
Cybersecurity Business Lead
geert.vander.linden@capgemini.com

**Secure Remote Working and Collaboration Solutions**

**Cybersecurity Services**

## References

1. CNBC, "Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems", March 2020
2. Reuters, "Mass move to work from home in coronavirus crisis creates opening for hackers: cyber experts, March 2020
3. ZDNet, "FBI re-sends alert about supply chain attacks for the third time in three months," March 2020
4. ZDNeT, "Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak", March 2020
5. CNBC, "Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems", March 2020
6. Cynet, "Recent Escalations in Cyberattacks in Italy Prove the Coronavirus Impact on Cybersecurity - Acting as a Warning for CISOs Worldwide", March 2020
7. Wired, "Hackers are targeting hospitals crippled by coronavirus", March 2020
8. TechRepublic, "667% spike in email phishing attacks due to coronavirus fears, March 2020
9. CISOMAG, "International Cybersecurity Experts Come Together to Fight COVID-19 Related Cyberthreats", March 2020
10. SC Magazine, "COVID-19 exposes gaps in cybersecurity safety net as millions work from home", March 2020
11. US Federal Bureau of Investigation's public service announcement, "FBI sees rise in fraud schemes related to the coronavirus (COVID-19) pandemic", March 2020
12. American Banker, "Bank CIOs confront challenge of so many employees working at home", March 2020
13. Forbes, "CIOs Vs. COVID-19: Tech Leaders Are Key To Companies' Emergency Plans," March 2020
14. Capgemini Research Institute, "Reinventing Cybersecurity with Artificial Intelligence", July 2019 report
15. AWS, "Siemens Handles 60,000 Cyber Threats per Second Using AWS Machine Learning," April 2019.
16. Capgemini Research Institute, "Reinventing Cybersecurity with Artificial Intelligence", July 2019 report
17. Gartner, "Preparing Your Security Operations for Orchestration and Automation Tools," February 2018
18. Capgemini Research Institute, "Reinventing Cybersecurity with Artificial Intelligence", July 2019 report
19. The Daily Swig, "Europol joins forces with European financial giants to tackle rise in organized cybercrime," March 2020
20. Capgemini Research Institute, "Reinventing Cybersecurity with Artificial Intelligence", July 2019 report
21. Barracuda, "Threat Spotlight: Coronavirus-Related Phishing", March 2020
22. Cmwire, "CIOs Share Business Continuity Plans Amid COVID-19 Pandemic, March 2020
23. GCN, "Cyber experts line up to defend medical community, critical infrastructure", March 2020
24. SC Magazine, "COVID-19 exposes gaps in cybersecurity safety net as millions work from home", March 2020
25. CIO, "COVID-19's impact on the enterprise and remote work," March 2020



# About Capgemini

Capgemini is a global leader in consulting, digital transformation, technology and engineering services. The Group is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year+ heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. Today, it is a multicultural company of 270,000 team members in almost 50 countries. With Altran, the Group reported 2019 combined revenues of €17billion.

Visit us at

**www.capgemini.com**

**People matter, results count.**



MACS_CS_20200401_AP