



CYBERSECURITY IN THE CONTEXT OF COVID-19

Businesses need to move quickly to ensure they protect against cyber threats as COVID-19 redefines how organizations operate around the globe.

The COVID-19 pandemic has redefined remote working mechanisms during a time of social distancing and working from home. These include but are not limited to:

 Increased use of mobile devices and digital collaboration tools for communication and handling of sensitive materials

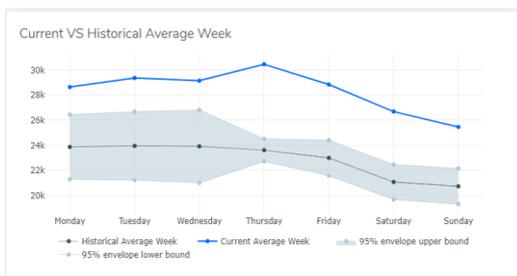
 Remote working arrangements, security tools, and corporate assets required to support.

Sia Partners discusses how key cyber threats have become more prevalent during COVID-19, and how companies can defend against these both now and in the aftermath of the pandemic.

Types of Cyber-threats on the Rise

The DDOS attack

A Denial of Service attack (a.k.a. DoS attack) is a computer attack designed to make a service unavailable for its legitimate users, usually by flooding the network with superfluous requests. The attack is called distributed (DDoS) when incoming traffic comes from multiple different sources. Observe the evolution of DDoS activity with respect Covid-19 worldwide on the dedicated Sia Partners dashboard at https://heka.sia-partners.ai/covid-19/cyber_security



Source: https://heka.sia-partners.ai/covid-19/cyber_security

The Phishing attack

A phishing attack preys on individual's trust of an organization through making a request or plea, or making an offer. Phishing takes many forms (such as spear phishing, whaling) but at a basic level, it usually takes the form of an email ostensibly originating from a trusted source, and may require the victim to click on a link or enter a password. At this point, the "phisher" will aim to extract sensitive information. Such attacks have become more prevalent across Asia, Europe, UK and the USA.

Remote working threats & attacks

- Remote working measures expose organization to a host of threats and attacks:
 - **Lack of sufficient additional layers of security** such as encrypted channel, and multi-factor authentication may expose an organization that has remote working arrangements, but has not taken into account the additional risk created through remote working. While cloud-based remote access vendors may provide some built-in security, organizations may be exposed unless they implement their own layers of protection.
 - **Insufficient visibility and patching protocols** in relation to personal devices being used for remote working create additional risk of exposure for organizations. Organizations may not be aware of the usage of personal devices, and even if they are, may not be able to mitigate the risk. This leaves organizations and the user of the personal device at risk of targeting by cyber attackers.

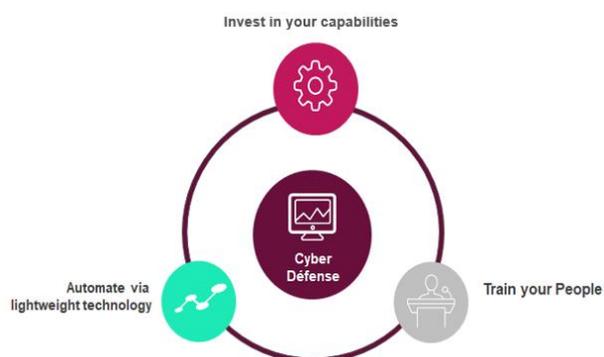
- **VPN Brute Force attacks** targets an organization's VPN usage for remote working distributing many authentication attempts using a previously acquired list of possible credentials to the VPN portal. If a permutation works, an attacker may gain access.
- **Man-In-the-Middle attacks** may take advantage of employees attempting remote access, via a threat actor creating a fraudulent login screen to steal credentials that would allow them to impersonate the user. Additional risk is created when employees work remotely by using personal Wi-Fi routers at home, which are easily hackable if they are not secured.
- **Insider threats** are more prevalent due to remote working, as employees may access sensitive data via an unsecured machine to perform tasks while not reliant on the network. Malicious employees may also attempt to steal data, made easier by the lack of visibility inherent in remote working. De-risking is more difficult if the user is able to access sensitive data via a personal device, due to a lack of IT security controls.

Securing Against the Cyber Threat

Borrowing from the comprehensive Sia Partners Resilience Capabilities, the following diagram summarizes key areas in protecting your business and your people against cyber threats:

1. Invest in your capabilities

According to cybersecurity solutions provider Fortinet¹, successful cybersecurity management involves quickly addressing vulnerabilities through proactive security



strategies, hygiene, and prioritization of threat intelligence.

Organizations should therefore:

- ☑ **Invest in building comprehensive databases** of vulnerabilities.
- ☑ **Stay informed** when a new vulnerability is discovered.
- ☑ **Perform severity assessments** to prioritize vulnerabilities.
- ☑ **Deploy patching plans** and collect KPIs for continuous compliance and measurement of effectiveness.
- ☑ **Implement physical measures** such as the blocking of USB ports of their devices to prevent data loss.

Examples of Cyber Attacks During COVID-19

In February 2020, a leading Singaporean bank's customers were targeted through a mobile app fraudulently made to look like an app the bank had released

In April 2020, customers of a global bank in Hong Kong received a phishing email asking them to click on a link and provide credit card details in order to receive aid during COVID-19

In April 2020, a Taiwanese bank advised its customers of an email posing as an email from the bank that requested customers to click on a link to a malware, posing as a PDF link

On March 18 2020, an existing Trojan "Trickbot" was detected using a brute forcing module that targeted financial services, education and telecom companies in Hong Kong and the USA

¹ Source: <https://www.fortinet.com/blog/partners/the-new-normal-how-service-providers-can-secure-their-customers-remote-workforces.html>

- ☑ **Implement Data Loss Prevention or Cloud Access Security Broker** solutions to protect data and ensure control and compliance regarding sensitive information.
- ☑ **Engage a proactive IT security team** to monitor security measures and act as incident management responders.
- ☑ **Strengthen security policies** to include:
 - enabling of multi-factor authentication across all network assets.
 - network segmentation to contain breaches.
 - strengthening passwords policy (e.g. require frequent renewal, exclusion of simple passwords, exclusion of repeat passwords).
 - hardening of remote access rules and procedures.
 - Enhancement of encryption protocols.
- ☑ **Measure response times** to any incident and collate the data for future responses.

These steps can help protect digital assets through improved security capabilities, continuous monitoring and updates with the latest protection, and use of lessons learned to more efficiently deal with future incidents.

2. Automate security tasks through lightweight technology

Take advantage of data science and automation to deploy bots to:

- ☑ **Automate tasks around identification, watchlist creation, and reporting** of key security vulnerabilities on an ongoing basis.

- ☑ **Generate severity assessments** that can be actioned by an organization's IT teams.

By automating simpler protection tasks, the organization can act faster to deploy key resources to manage an incident, while freeing up an IT team to conduct more complex tasks during non-incident periods.

3. Invest in your people

According to cyber security solutions provider Palo Alto², organizations that provide training as well as improve their cyber-security infrastructure are more efficient in defending against attacks.

It is essential that staff:

- ☑ **Are aware** of the potential cyber threats they are exposed to.
- ☑ **Have the knowledge** on they can mitigate the risk.
- ☑ **Feel empowered** by company policy to take action.

By investing in comprehensive and ongoing security awareness training (not just the yearly compliance training) for employees who are working from home, working out of office, or who have access to sensitive documentation, an organization can complement its technological efforts through molding employees into competent and confident threat assessors.

²Source: <https://blog.paloaltonetworks.com/2020/04/network-working-from-home/>

How Sia Partners Can Add Value to Your Cybersecurity Efforts

Leverage our global security capabilities to help your organization define, execute and monitor your security strategy for COVID-19 and beyond.



COMPREHENSIVE SECURITY SERVICES

Utilize our services across cybersecurity strategy, risk management, compliance, operations, and resilience to implement the right measures to protect your organization.



DATA DRIVEN THREAT MANAGEMENT

Implement **our ready-to-deploy cyber-security** bot to automate threat management across the following areas:

- Build a comprehensive database of vulnerabilities from different sources
- Match all variants of a software name input, with the standardized names from a comprehensive and updated vulnerability database
- Do basic data quality to identify the versions provided even when the name or version of the software is incomplete
- Define a watchlist and alert settings to be informed immediately when new vulnerabilities are discovered and might affect IT assets
- Autonomously categorize all IT assets into asset and generate a report with different views and breakdowns.
- Perform a severity assessment and prioritize vulnerabilities according to a finely tuned severity score.



SECURITY AWARENESS TRAINING

Engage, educate, and empower your staff to prevent, detect, and confidently act when faced with a cyber risk through our on-site workshops or conference-based security awareness training, led by security specialists and experienced trainers.

YOUR CONTACTS

STEFANO FOIS

Senior Manager, CIO Advisory
+952 9723 3483
stefano.fois@sia-partners.com

VINCENT KASBI

Head of Asia
+852 6800 5988
vincent.kasbi@sia-partners.com

DAVID HOLLANDER

Partner, Singapore
+65 8112 5823
david.hollander@sia-partners.com

ABOUT SIA PARTNERS

Sia Partners is a next generation consulting firm focused on delivering superior value and tangible results to our clients as we navigate the digital revolution. Our global footprint and our expertise in more than 30 sectors and services allow us to enhance our clients' businesses worldwide. We guide their projects and initiatives in strategy, business transformation, IT & digital strategy, and Data Science. As the pioneer of Consulting 4.0, we develop consulting bots and integrate AI in our solutions.



Abu Dhabi | Amsterdam | Baltimore | Brussels | Casablanca | Charlotte | Chicago | Denver | Doha
| Dubai | Frankfurt | Hamburg | Hong Kong | Houston | London | Luxembourg | Lyon | Milan |
Montreal | New York | Paris | Riyadh | Rome | Seattle | Singapore | Tokyo | Toronto | Greater Bay
Area | Panama City (*Sia Partners Panama, a Sia Partners member firm*)



For more information, visit www.sia-partners.com

Follow us on **LinkedIn** and **Twitter @SiaPartners**