Deloitte.

Holistic view on cyber risk
in the pandemic era

Extraordinary times call for extraordinary measures

COVID-19, also known as the coronavirus, recently created a **disrupted environment** for many public and private organisations across the globe. In different order of magnitude, governments took action to contain this viral threat from spreading in their countries, including limiting physical movement, self-quarantine, and encouraging teleworking. With these **new measures** came new challenges for the business continuity of many public and private organisations. Many businesses were forced to reinvent themselves and adapt their way of working to a **new reality** without prior warning. For example, organisations had to accommodate for a changing supply chain, new communication channels, a new approach for talent and sales, and many other business aspects. On top of that, the security and continuity of IT infrastructure and services are more critical than ever as the dependency on digital tools has significantly increased. **Cyber is everywhere so society can go anywhere**. However, the technology used nowadays often lacks the maturity to ensure proper security and privacy of all re-invented business functions. Therefore, it is now essential for businesses to empower their CISOs and DPOs to allow the organisation to adapt to the changed work environment.

Indeed, the disrupted landscape calls for a **review of existing measures**. Not only because of how employees' **work environment** changes, but also since an organisation's focus shifts to adapt to the **evolved threat landscape**.

Proliferation of threats on remote workers and communication platforms

By encouraging people to work from home as much as possible, the life of many has changed. This change also created **new social challenges** for the population. For some people, self-quarantine means self-isolation, for others it means the need to rigorously split time between work and private life to keep things in balance as both happen at home. In times of crisis and isolation, people need to find ways to manage their time and keep physically and mentally healthy, while cyber security might become a lesser concern. However, as communication and information sharing currently mainly relies on digital tools and platforms, staying in control of **cyber risks has become a business imperative**.

Using home Wi-Fi networks for professional activities is a hurdle in itself as these bandwidth plans usually have much lower capacity than in the workplace. Additionally, when a single network is used by a few people in the house at the same time, it can cause congestion and reduced speed. Moreover, home networks might not be as secure as company networks and malicious entities could get in the way between employees and their company to run a "Man-in-the-Middle" attack that can intercept business confidential data leading to even more damages to companies.

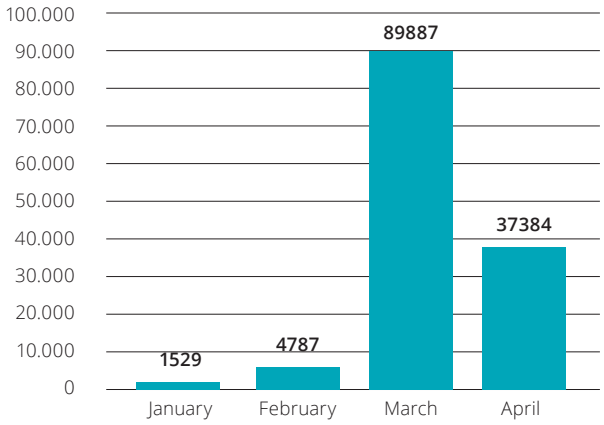
Another essential point lies in the evolution of our environment. As the line between personal and work environments becomes flimsy, corporate devices can become household items and parents may allow their kids to use those for recreational or learning purposes. The extended use of corporate devices for personal and recreational purposes introduces new cyber risks for many companies. For example, "phishing" attempts, which aim at impersonating one's corporate identity or device to trick victims into sharing resources, could lead to the leakage of confidential data and to the disruption of critical business activities. Forged mails from CEO's sending links with guidelines (linked to COVID-19) are the phishing technique which has increased the most during the pandemic era. While it may be tempting to solely rely on technical measures, increased user awareness and training remains an important barrier when enforcing security in an environment that proves harder to monitor. To this end, parents could educate their children in a "tech savvy" way allowing a higher security level when working from home.

Deloitte Cyber Threat Intelligence (CTI) looked at the number of fake or "spoofed" websites, impersonating official coronavirus information sources or healthcare organisations, created to steal data or deliver payloads with malicious purposes on a victim's machine, for example to gain remote access and steal banking information. The number increased from less than 50 in November 2019 to more than 11 000 in mid-April 2020. These numbers prove that attackers are well aware of this empowered attack vector and are widely exploiting it.

Employees may also use their personal email or private devices to exchange business related information, especially employees whose companies were not used, nor prepared to work remotely. It is possible that employees have to resort to those devices and channels when working from home. These unmanaged – and maybe unsecured – devices and channels could cause **integrity and availability** problems for businesses, as they could lead to data leakage, disruption of activities or worse, access to the company network.

On top of this growing threat, the physical environment we work in nowadays could also lead to **confidentiality** issues as cohabitants might overhear business conversations including confidential information without knowing what shouldn't be disclosed and this too could lead to the leakage of confidential business information.

Number of malicious websites related to Covid-19



This graph provides insights in the rise of the number of malicious websites related to COVID-19 over the past few months. The data was collected from domaintools.com and represents the websites that have been assigned a risk score of more than 70/100. The risk score predicts how likely a domain is to be malicious.

What does this mean for your organisation?

The migration of employees from the corporate office to the home office introduces some **short and long-term challenges for organisations**. The novel coronavirus pandemic has produced greater demands on remote work infrastructures and digital customer experiences. This forces businesses to rethink their approach to technology and the role cybersecurity should play in empowering their underlying business objectives.

In the **short term, three primary drivers** contribute to elevate threat levels that executives can prepare to address throughout their organisations.

The pandemic has created the opportunity for malicious actors to **exploit vulnerabilities** and take advantage of widespread disinformation and fears around the pandemic. Attacks such as clickbait, social engineering schemes, and disinformation campaigns are increasing, and in many cases are effective. Cyber attackers need only a small window of opportunity to entice an employee to open a corrupted attachment or click on a hostile link that can embed a threat in an environment and wreak havoc immediately or in months to come.

A shift in remote work arrangements combined with staff disruptions is testing the **bandwidth** of virtual private networks (VPNs) and other security controls for many organisations. While remote access may have been previously supported and controlled, the sheer volume and frequency of demands on infrastructure test the integrity of governance mechanisms. For organisations that did not support home work in the past, this change dictates support for securing and monitoring home or personal networks.

On top of this, many companies are relaxing their **risk tolerances** with respect to third parties. This may affect a company's extended defences against cyber risk, as many companies are shifting to contingency providers. Due to the changed environment, third parties are forced into alternate delivery patterns and they may not ensure the same security coverage, which may lead to increased overall digital risk.

Besides addressing near-term cybersecurity risks, organisations may want to start considering **future scenarios** as the pandemic continues to affect day-to-day efforts. Companies may need to establish and maintain a framework to continually measure critical risk indicators and prepare protections for controllable and foreseeable uncertainties. This approach enables businesses to capture the lessons in the early stages of the COVID-19 outbreak and apply them in the future.

In the **long term**, organisations may face concerns such as **reduced budgets and under-resourcing** of information security functions, which may lead to a greater digital risk. Next to this, threats from earlier opportunistic attacks are likely to remain hidden in the environment, which creates sustained increased risk to an organisation's infrastructure and data.

Companies may also witness an increase in **opportunistic mergers and acquisitions** as long term economic dynamics may lead to opportunistic mergers and acquisitions that move quickly and do not include sufficient cyber due diligence.

Finally, companies should be careful with **employment shifts and workforce reorganisations** as disturbances to normal business cycles might lead to inadvertent insider threats posed by disgruntled employees.

What can you do to mitigate these risks in this pandemic era?

First of all, it is clear that organisations need to **reprioritize** their cybersecurity strategy and take action to boost cyber defences. Instead of focusing too much on business-critical processes that may require urgent attention, organisations should also prioritize cyber risk in order to ensure that they can lead resilient businesses in the future, once the pandemic chaos has settled.

Organisations can consider **several steps** to build their cybersecurity and address the abovementioned near- and long-term challenges.

Companies should **strengthen threat intelligence programs** and integrate them with other critical activities, such as security event monitoring. They should also ensure active vulnerability discovery and threat hunting.

Next to this, it is important for organisations to maintain **proactive communication** with employees and third parties in order to raise awareness on cyber threats and ensure prevention of such threats. Engage your workforce on the security implications of working from by explaining and educating them on best practice concerning remote working, for example sharing files securely, connecting to the corporate network via VPN, and using secure passwords. To facilitate these best practices, organisations should ensure secure remote access with the review of VPN governance security posture and the use of multi-factor authentication.

Organisations should also update their **security incident response playbooks** and create an after-action report. Documenting response activities taken in this pandemic crisis, including identified gaps and areas for improvement may produce useful insights and lessons learned for future situations.

Lastly, organisations should **strengthen security in high risk areas**, for example by updating their security architecture and ensuring coverage for insider threat and cyber diligence. In addition, organisations should consider accelerating the implementation and optimisation of critical security solutions, such as multifactor authentication or mobile device management, especially for high-risk applications or connectivity platforms.

What if your systems get compromised anyway?
In case a cyber-attack succeeds, despite all security measures taken, organisations will need to follow a step-by-step approach to recover their critical business operations. First of all, key systems need to be isolated for protection. Second, the organisation needs to fully understand and contain the incident, and consequently, eliminate any malware. Afterwards, appropriate protection measures should be implemented in order to improve the overall system posture, and identify and prioritise recovery of its key business processes to deliver operations. Finally, the organisation should implement a prioritised recovery plan.

What if your systems get compromised anyway?

In case a cyber-attack succeeds, despite all security measures taken, organisations will need to follow a **step-by-step approach** to recover their critical business operations. First of all, key systems need to be isolated for protection. Second, the organisation needs to fully understand and contain the incident, and consequently, eliminate any malware. Afterwards, appropriate protection measures should be implemented in order to improve the overall system posture, and identify and prioritise recovery of its key business processes to deliver operations. Finally, the organisation should implement a prioritised recovery plan.

Looking at the coronavirus crisis, we can say that the dependency on digital tools has significantly increased and that the impact of cyber-attacks has amplified. Incorporating cyber strategies into current crisis response planning is important so that cybersecurity remains closely connected with agile business processes, human resources management, and information technology. It is most critical for businesses to review their current situation, in particular to reassess remote access and employee awareness, and to rethink their cyber strategy while closely monitoring all activities going in and out the corporate network. The most important things to do right now is to educate employees on cyber threats related to working from home, patch and review your corporate systems, set up the tools to detect intrusions and be ready to respond to a potential security incident or personal data breach.

Our services

Cyber Fusion Services
- Security monitoring
- Threat intelligince
- Attack surface management
- Threat hunting
- Data loss prevention

Incident Response (IR) & Business Continuity
- IR plans and retainers
- Digital forensics, malware, and threat analysis
- Breach impact analysis
- Business continuity and Technical resilience plans

Awareness & Training Programs
- Phising awareness
- Training campaigns
- Enterprise communications

Identity and Data Protection
- Identity governance
- Acces management
- Risk-based authentication
- Data governance
- Data privacy (e.g., GDPR compliance)

Other considerations

Overall Security programs and risk tolerances:

- Scaling of security systems & processes
- Increased attack surface area
- Identity governance controls
- New hires & terminations
- Incapability of remote work
- Cloud security to support e-commerce
- BYOD & non company-issued device risk
- Complexities for power & utilities
- Privacy implications of employee health monitoring

For government and public services:

- Monitoring for emerging cyber schemes to steal citizen identities and defraud government tax and benefits agencies
- Refresh alternatives for securing sensitive activities (e.g. mobile Sensitive Compartment Information Facilities (SCIFs), remote verification of identities to process clearances, hard tokens)
- Adopt new methodes for students, faculty, and administrators to conduct transactions (e.g., secure testing, research lab security)

Deloitte.