WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust

Cybersecurity Leadership Principles

Lessons learnt during the COVID-19 pandemic to prepare for the new normal

May 2020

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Introduction

The world is experiencing an unprecedented crisis that is causing chaos in the global economy, disrupting supply chains and transforming society. The new reality is accelerating business model transformation at a faster pace than ever before to ensure existential survival in a crisis for which no one was prepared.

The COVID-19 pandemic is having a dramatic impact on society and has forced everyone to become heavily reliant on the internet and its digital economy – what would normally have taken years has now occurred in months. The situation has highlighted the intrinsic systemic issues at the juncture of digital infrastructure, economy, geopolitics and privacy that mainly relate to the unprecedented pressure on the digital architecture and supply chain dependencies. If these are not addressed in a holistic manner, the escalating risks may have a domino effect that is likely to impact critical functions and industry ecosystems globally.

The large-scale adoption of remote-access technologies to enable work-from-home practices, with greater reliance on cloud services, enables companies to continue operations and reduce costs in conditions of social distancing and “stay-at-home” orders from government and/or employer. It is also reshaping the digital landscape and architecture while straining supply chain resiliency and cybersecurity operations with the escalating risk.

This confluence of forces is likely to impact critical functions and the broader industry ecosystems globally:

- Working from home or remotely has increased the attack surface exponentially and multiple vectors for cyberattacks through the heightened dependency on personal devices and residential networks
- Social engineering tactics remain very effective on a workforce that is distracted and vulnerable
- Maintaining the cyber resilience of a highly interconnected supply chain becomes even more challenging
- Rapid deployment of new services, mostly cloud-based, and changes to the network architecture may bypass important risk-assurance steps and expose the broader ecosystem
- Critical business assets and functions are significantly more exposed to opportunistic and targeted cyberattacks by criminal organizations and nation states seeking to take advantage of rising vulnerabilities
- Essential critical infrastructure services, such as hospitals, are under acute pressure and have been hit particularly hard by new forms of ransomware aimed at disrupting vital services

It is imperative that leaders strategically manage information risks, work towards a culture of shared cyber-risk ownership across organizations and take a strategic approach to cyber resilience. Effective cyber resilience requires a combined and aligned multi-disciplinary effort to move beyond compliance to cohesive business and digital enablement.

Businesses need to consider cyber resilience from a business perspective, looking at the cyber element of operational risks to their business as they become increasingly dependent on the internet and digital channels. They also need to adopt a resilience mindset of how they would respond to and recover from any major cyber event.

The following principles will help organizations to shape a responsible course of action that balances short-term goals against medium- to longer-term imperatives:

1. Foster a culture of cyber resilience

Resilience is first and foremost a leadership issue and is more a matter of strategy and culture than tactics. Being resilient requires those at the highest leadership levels to acknowledge the importance of proactive risk management and focus more on the ability of the organization to absorb and recover from a cyberattack that would disrupt essential services.

2. Focus on protecting your critical assets and services

Businesses will have to prioritize resources and investments to the most essential areas to maintain operational continuity, protect the critical digital assets and ensure compliance.

3. Balance risk-informed decisions during the crisis and beyond

Businesses are making changes to their operating model and technology landscape at an unprecedented scale and pace, which will require some risk trade-offs as they adapt and respond urgently to the crisis. However, as they enter the new normal, they will need to reassess the digital dependencies and risks accrued to restore their risk profile to an acceptable level.

4. Update and practice your response and business continuity plans as your business transitions to the new normal

This crisis has reminded business leaders of the importance to adapt and test regularly their response and resilience plans against different disaster scenarios (including pandemics) with their key suppliers and business partners. This includes using these tests to challenge assumptions (such as recovery times) and to develop means to measure resilience, response, recovery and other key capabilities needed to anticipate, withstand and recover from, and adapt to, adverse conditions, attacks or compromises on systems that are enabled by cyber resources.[1]

5. Strengthen ecosystem-wide collaboration

Partnerships and collaborations on cyber resilience between public and private sector peers across the ecosystem are essential in facilitating the transparent sharing of information and go beyond subscription towards a more active engagement.

The principles in this document are a preliminary response to the unfolding crisis. They are intended to guide leaders specifically responsible for cyber resilience, and other business leaders. While businesses may have to regulate measures according to different policy environments, these concepts can provide a framework for a responsible course of action at this pivotal period.

Cybersecurity Leadership Principles

1. 

   Foster a culture of cyber resilience

2. 

   Focus on protecting critical capabilities and services

3. 

   Balance risk-informed decisions during the crisis and beyond

4. 

   Update and practice your response and business continuity plans as your business transitions to the new normal

5. 

   Strengthen ecosystem-wide collaboration

1. Foster a culture of cyber resilience

The COVID-19 crisis has highlighted that focusing only on cybersecurity is insufficient if the challenges of digitalization are to be effectively met. Protection and defence strategies are important but businesses must also develop strategies to ensure resilient and sustainable networks while taking advantage of the opportunities that digitalization can bring. Additionally, since a vulnerability in one area of the supply and value chains can compromise the entire organization, resilience requires a conversation focused on critical systems and processes rather than a blanket approach.

The following key actions will help leaders instil a culture of cyber resilience within the enterprise and broader ecosystem:

Implement cyber-resilience governance

Cyber resilience is a business issue that affects all aspects of the organization. The board must take responsibility of its oversight and instilling the cultural shift that must take place.[2] Furthermore, implementing a comprehensive cyber-resilience governance by appointing an accountable officer should break down the barriers between business, IT, OT and physical security and business groups, facilitate the development of cyber skills and capabilities and institute an appropriate structure to ensure a coordinated cyber-resilience strategy and priorities across the organization's response to the COVID-19 crisis.

Promote resilience by design

Cyber risks and implications should, from the outset, be monitored and managed proactively across IT and business process changes, mergers and acquisitions and third-party engagements.[3] This will ensure that businesses identify cyber risks that need mitigation upfront and manage the cost of these initiatives accordingly. It will also enable them to take advantage of the business efficiencies that digitalization offers while controlling the associated cyber risks and impact.

Go beyond compliance

Given the numerous regulations and compliance requirements in several essential critical infrastructure sectors, cyber-resilience efforts often take on a "check-the-box" mindset. However, the digital ecosystem is a dynamic environment in which cyber threats often evolve faster than regulation. During this pandemic, businesses may need to prioritize business continuity, incident response and recovery activities and work with their regulators to define a reasonable timeline to restore their organization compliance state to an acceptable level.

Strengthen cyber-resilient employee behaviours

Every day, employees make decisions that can have as much impact on security as technical controls. Keeping an organization secure is every employee's responsibility. Front-door attack vectors such as phishing emails, for example, are used by many criminal organizations. The number of phishing emails has soared during the pandemic, and scammers impersonating World Health Organization (WHO) employees have targeted relief funds for COVID-19 victims and lured users to malicious websites using fake advertisements. Businesses should help employees stay secure through regular training to identify suspicious emails as well as keeping them informed on the latest techniques that may arise during a crisis. Furthermore, applying the principle of least-privilege access and having advanced anti-malware and anti-phishing capabilities will reduce significantly the exposure to phishing campaigns.

2. Focus on protecting critical capabilities and services

Business leaders must have a holistic and systemic view of their critical services, applications, suppliers and assets to determine the potential ramifications of a crisis to revenue, employees, customers and continuity of essential services. Cyber health has many similarities to human health and a parallel could be drawn between the preventive, tracing and response measures to the COVID-19 virus and those recommended for digital viruses.

The following key actions will help leaders maintain the cyber health of their businesses and protect capabilities and services that are critical to operations.

Enforce strong cyber hygiene

Effective and consistent implementation of strong cyber hygiene would have mitigated the majority of the cyberattacks of the past decade and many of the attacks that were perpetrated since the beginning of the pandemic. Exploitation of known vulnerabilities that exist on a server, application or endpoint device are common entry points for a cyberattack. Developing and maintaining an inventory of all digital assets starting with the critical ones will help ensure an effective vulnerability management strategy and will be essential in protecting critical systems against cyber threats.[4]

Protect the access to critical assets

Businesses will need to invest in enhanced identity and access management systems to meet new “perimeter-less” challenges posed by the rapid shift to remote working. Implementing network segmentation and strong authentication measures with automated systems to provision and revoke entitlements is an imperative. There must be a layered access mechanism for privileged users to gain access to a mission-critical system. To secure remote connectivity, businesses should deploy layered defence-in-depth to prevent data leaks and detect suspicious activities from endpoints connected remotely (e.g. VPN using multifactor authentication).

Monitor abnormal activities on your critical assets

Businesses should consider increasing investments in monitoring and response capabilities to help decrease the detection-to-mitigation time. This can include remote monitoring of collaboration tools, monitoring networks for new and novel strains of malware, as well as monitoring employees and third parties to catch abnormal activities before they result in operational outages or subversive activity.

Prioritize investments in cybersecurity automation

In the current digital economy, businesses will have to allocate limited resources wisely and invest in technologies such as artificial intelligence (AI), machine learning (ML) and big data to automate mundane cybersecurity processes and minimize the risk of human error. These processes would include, for instance, the provisioning and revocation of entitlements to ensure appropriate access rights to access critical services and sensitive information, the scanning of vulnerabilities and triage of the different security events and anomalies. As a result, businesses will be able to reassign their resources in other important activities related to process improvement, incident response and new threat scenarios preparedness.

3. Balance risk-informed decisions during the crisis and beyond

Business leaders should recognize that their business risk posture has changed significantly and will need to be restored to an acceptable level after the crisis. The following key actions will help leaders balance risk-informed decisions:

Move towards a zero-trust approach to securing your supply chain

The high velocity of new applications being developed alongside the adoption of open source and cloud platforms is unprecedented. Organizations often fail to resolve bugs or configuration issues for their software applications, as was the case for Zoom, which has been under a lot of scrutiny during the pandemic for security and privacy flaws. As hackers are proactive in identifying and exploiting the weakest link in a value chain, a zero-trust approach to securing the supply chain must become the norm.

Define and implement meaningful cyber-resilience metrics

To effectively integrate cybersecurity and resilience into business strategy, monitoring cyber resilience and risks efforts, as well as measuring the effectiveness of investments and capabilities, are essential for business stakeholders to make informed decisions. Technical cybersecurity metrics are often measured and reported, but they need to be aligned with business strategic objectives and translated into a standard format that decision-makers can understand and act on. Businesses should develop quantitative and qualitative metrics for detection, response, containment and recovery capabilities, and use tests and exercises to apply these metrics. For instance, a dashboard could capture critical dependencies for systemic resilience and the exposure of business processes to a variety of risks and resilience issues.

Focus on cyber risks critical to operations

Business leaders need to understand the implications of the COVID-19 pandemic on digitalization strategies and prioritize technologies, security capabilities and service rollouts that are critical to operations. With new vulnerabilities and risks growing rapidly due to the fast pace of change in technology, leaders will have to prioritize and manage those that represent the highest criticality to business operations.

4. Update and practice your response and continuity plans as your business transitions to the new normal

While many cyber-resilience leaders and other business leaders have drawn on their experiences of past crises to respond to the early stages of the COVID-19 outbreak, the pandemic's scale and unpredictable duration make the response and recovery efforts particularly difficult.

The following key actions will help leaders maintain business continuity in this turbulent and dynamic period:

Practice a comprehensive crisis management plan

Crisis management is a critical component of any business continuity programme, where a major disaster or incident is not a matter of if, but when. An organization that focuses solely on analysing and mitigating risks may not be well-positioned to manage a crisis. Thus, building a cross-functional team with the aptitude for crisis management is the first building block. When a crisis such as this pandemic occurs, a highly detailed plan is invaluable in orienting individuals with different roles and responsibilities towards a common goal and collective action. Such a plan needs to span the entire spectrum of company activity, ranging from the tools to be used for case management and internal communication to the key contacts with government agencies, law enforcement, legal and insurance experts in case of need to communicate with these parties.

Maintain and adjust response and resilience plans

Management should test and continuously improve incident response, disaster recovery and business health continuity plans, including cyberattack and pandemic scenarios to maintain a state of response readiness. These plans should balance preparedness and protection (e.g. defence in-depth strategies) with response and recovery capabilities to maintain business continuity during this crisis and beyond. Businesses must determine whether their organization's risk-response approach is effective and efficient.

Prepare for the new normal

As we look beyond the COVID-19 pandemic, organizations need to prepare for new methods of engaging with their use of technology.

Remote working from home continues
With the shift to working from home during the pandemic, businesses will likely extend it to reduce operating costs. They should be prepared to continue offering secure remote technologies powered by cloud computing that strikes a balance between security, user experience, cost and efficiency.

Digitalization will keep accelerating
During the pandemic, all businesses are undergoing transformative digitalization that will change their digital architecture and technology at an unprecedented pace. This digital transformation is powered by technologies such as AI, cloud computing and the internet of things, and will connect everything from assets to people and data. The cyber-risk management practices should adapt with agility and speed to the new business context to ensure alignment with strategic business priorities and risk appetite.

5. Strengthen ecosystem-wide collaboration

Public- and private-sector leaders need to promote collaboration and actively participate in initiatives to ensure that actions are taken to secure the broader ecosystem against current and emerging cyber threats. Furthermore, businesses must align expectations with suppliers on their cybersecurity controls (and associated compliance regimes) to encourage regulatory alignment in terms of third-party assurance, and also take forward a range of community initiatives to raise awareness of cybersecurity risks within the broader supply chain.

The following key actions will help leaders instil a culture of collaboration within the enterprise and across the ecosystem:

Increase collective situational awareness

The distributed nature of many digital ecosystems may make it difficult for a single organization to efficiently identify a cyberattack. Overcoming this challenge requires a real-time, transparent sharing of information to build collective situational awareness. Moreover, the sharing of real-time information should take into account national security implications as information to manage cyber risks will need to cross national and regional boundaries. A key element in fuelling information sharing is to increase regulatory protection for victims to incentivize the affected parties to share information on cyberattacks and breaches without fear of repercussion. Knowing the key government agencies and personnel in the jurisdictions in which business is conducted is also essential. Law enforcement and the government can be key partners in prevention as well as in response during any crisis such as this pandemic.

Drive collective action

This collaboration must go beyond subscription to information feeds and include active participation in industry action groups which should strive to coordinate actions against cyber-criminal groups and nation-state actors, thus having a more strategic impact on adversaries by sharing curated cyber threat intelligence specific to an industry. For instance, several alliances such as the Cyber Threat Alliance, CTI League and COVID-19 Cyber Threat Coalition include thousands of industry experts working with law enforcements and governments to accelerate the sharing of actionable information to fight cyber-criminal activities targeting essential services such as hospitals.

Take a systemic approach to cyber-risk management

Every connected device represents a potential entry or execution point for a cyberattack. Both the organization's assets and interdependence with the broader ecosystem needs to be assessed. However, the ecosystem needs to be mapped by prioritizing dependencies based on the business and cyber risk they pose. This is especially critical when it comes to the supply chain. Risk assessments need to explicitly quantify supply chain cyber risks and evaluate whether the processes in place to manage such risks are robust and effective. Without a common understanding and systemic approach to cyber risks, businesses will struggle and even fail in implementing appropriate countermeasures to mitigate them. It is crucial for all stakeholders in the value chain to embrace a collaborative and risk-informed cybersecurity approach to adapt and ensure a secure ecosystem.

The New Normal

The COVID-19 crisis has generated unprecedented challenges to organizations, forcing everyone to juggle professional responsibilities with important personal ones. The coming months are likely to bring more uncertainty. By adhering to the practices proposed, business leaders can better meet their responsibilities to uphold their organization's security posture and maintain business continuity during this pandemic and beyond. With effective cyber-risk management and cyber-resilience practices, businesses can achieve smarter, faster and more connected futures, driving business growth and efficiency.

As the cyber threats to business continue to evolve, public- and private-sector leaders will have to address them in the digital and physical worlds to mitigate any potential harm to individuals and avoid the disruption of critical services. Businesses that understand and act on the signals and warnings can adapt and turn an increasingly ambiguous and fast-moving world to their advantage.

Contributors

Lead Author

Georges de Moura	Head of Industry Solutions, Platform for Shaping the Future of Cybersecurity and Digital Trust, World Economic Forum

Contributors

The World Economic Forum thanks the following individuals for participating in interviews, workshops and discussions that contributed to the development of this white paper.

Sandro Bucchianeri	Group Chief Security Officer, Absa Group, South Africa
Rob Wainwright	Partner, Cyber Risk Services, Deloitte, Netherlands
Chris Verdonck	EMEA Cyber Risk Services Leader, Deloitte, Belgium
Mark Hughes	Senior Vice-President Security, DXC Technology, UK
Kris Lovejoy	Global Advisory Cybersecurity Leader, EY, USA
Elizabeth Joyce	Senior Vice-President & Chief Information Security Officer, Hewlett Packard Enterprise, USA
Drew Simonis	Vice-President, Deputy Chief Information Security Officer, Hewlett Packard Enterprise, USA
Vishal Salvi	Chief Information Security Officer, Infosys, India
David Ferbrache	Global Head of Cyber Futures, KPMG, UK
Rajiv Singh	Head of Cybersecurity, Tech Mahindra, India
Dhaval Bhatt	Global Business Development Cybersecurity, Tech Mahindra, India
Greg Day	Vice-President and Chief Security Officer EMEA, Palo Alto Networks, UK
Haider Pasha	Chief Security Officer Emerging markets, Palo Alto Networks, UAE
Hisham A. Al-Muhareb	Head of Information Security Governance, Saudi Aramco, Saudi Arabia
Wesam A. Alzamil	Global Cybersecurity Governance Specialist, Saudi Aramco, Saudi Arabia
Khalid Al-Harbi	Chief Information Security Officer, Saudi Aramco, Saudi Arabia
Yasser N. Alswailem	Vice-President, Cyber Security, Saudi Telecom Company, Saudi Arabia
Charles Blauner	Partner & CISO in Residence, Team8, USA
Neal Pollard	Chief Information Security Officer, UBS, Switzerland

The Forum also wishes to acknowledge the contribution of **William Dixon**, Head of Future Networks and Technology and **Nayia Barmpaliou**, Head of Public Policy and Initiatives, Platform for Shaping the Future of Cybersecurity and Digital Trust, World Economic Forum.

Endnotes

1. National Institute of Standards and Technology. 2019. *Developing Cyber Resilient Systems A Systems Security Engineering Approach.* https://csrc.nist.gov/CSRC/media/Presentations/developing-cyber-resilient-systems/NIST%20Cyber%20Resiliency%20Presentation.pdf (Link as of 22 May 2020)

2. World Economic Forum. 2017. *Advancing Cyber Resilience: Principles and Tools for Boards.* https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards (Link as of 22 May 2020)

3. World Economic Forum. 2019. *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards.* https://www.weforum.org/whitepapers/cyber-resilience-in-the-electricity-ecosystem-principles-and-guidance-for-boards (Link as of 22 May 2020)

4. World Economic Forum. 2019. *The Cybersecurity Guide for Leaders in Today's Digital World.* https://www.weforum.org/reports/the-cybersecurity-guide-for-leaders-in-today-s-digital-world (Link as of 22 May 2020)

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744

contact@weforum.org
www.weforum.org