WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust

The Cybersecurity Guide for Leaders in Today's Digital World

October 2019

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

Foreword

Rob Wainwright
Senior Partner
Deloitte

I am delighted to introduce this important guide, which is the product of a joint collaboration between the World Economic Forum and several of its partners. The cybersecurity challenges confronting all companies in today's interconnected digital economy have reached new levels of complexity and scale. The threats are propagated via innovative new forms of malware, through the compromise of global supply chains and by sophisticated criminal and hostile state actors. These and other characteristics are at the heart of an expanding cyber-criminal economy that is difficult to counter.

Cyber is everywhere and it is here to stay. Global companies realize that they can no longer buy their way out of cyber challenges nor find a silver bullet by which to remove the threats. Developing more robust levels of cyber resilience is now the order of the day, and this is as much about developing a new culture and mindset as it is about adopting different processes and technology. The cyber imperative brings new demands on those responsible for running the business of cybersecurity in companies and organizations.

This guide is therefore timely and welcome as it charts the key tenets of how cyber resilience in the digital age can be formed through effective leadership and design. From the steps necessary to think more like a business leader and develop better standards of cyber hygiene, through to the essential elements of crisis management, the guide offers an excellent cybersecurity playbook for leaders in this space. Based on my long experience of working in the intelligence and law enforcement communities, as well as my current exposure to the boards and executive teams of many global companies as a partner of Deloitte, all the elements herein are relevant and timely.

The recommendation to foster internal and external partnerships is one of the most important, in my view. The dynamic nature of the threat, not least in terms of how it reflects the recent growth of an integrated criminal economy, calls on us to build a better global architecture of cyber cooperation. Such cooperation should include more effective platforms for information sharing within and across industries, releasing the benefits of data integration and analytics to build better levels of threat awareness and response capability for all. Technology solutions and governance models are available to meet this goal, all within strong and responsible conditions of data privacy and security.

In this and other priority areas highlighted here we require public- and private-sector leadership to drive this important change. It will take us to a better, more confident cyber future. For the cyber security leaders involved, reading this guide is a great way to start.

Executive Summary

Cyberattacks are one of the top 10 global risks of highest concern for the next decade, according to the World Economic Forum *Global Risks Report 2019*, with data fraud and theft ranked 4th and cyberattacks 5th. Globally, their potential cost could be up to $90 trillion in net economic impact by 2030[1] if cybersecurity efforts do not keep pace with growing interconnectedness, according to the Atlantic Council and the Zurich Insurance Group, among others. Although government and corporate leaders are deeply engaged in promoting effective cybersecurity strategies and the global spending on security continues to accelerate, the annual number of cyberattacks globally hit an all-time high last year.

Top 10 risks in terms of
Likelihood

1. Extreme weather events
2. Failure of climate-change mitigation and adaptation
3. Natural disasters
4. Data fraud or theft
5. **Cyberattacks**
6. Man-made environmental disasters
7. Large-scale involuntary migration
8. Biodiversity loss and ecosystem collapse
9. Water crises
10. Asset bubbles in a major economy

Top 10 risks in terms of
Impact

1. Weapons of mass destruction
2. Failure of climate-change mitigation and adaptation
3. Extreme weather events
4. Water crises
5. Natural disasters
6. Biodiversity loss and ecosystem collapse
7. **Cyberattacks**
8. Critical information infrastructure breakdown
9. Man-made environmental disasters
10. Spread of infectious diseases

Figure 1 – *Global Risks Report 2019*

There is an abundance of guidance in the cybersecurity community from well-accepted government and industry standards for information security globally, including ISO, NIST and many others. Yet the application of the guidance continues to fall short of what is required to ensure effective defense against cyberattacks. The World Economic Forum Centre for Cybersecurity has worked with its partners to consider the current barriers to the adoption of these practices in an effort to provide some key essentials to organizations wishing to improve their ability to defend against attacks.

This guide is intended for senior executives who are responsible for setting and implementing the strategy and governance of cybersecurity and resilience in their organization. Cybersecurity is everyone's responsibility in an organization, not solely of the Chief Information Security Officer. It is essential that key stakeholders in the C-Suite, such as Chief Information Officers, Chief Technology Officers, Chief Digital Officers, Chief Financial Officers and other company executive officers understand their responsibilities as it relates to cybersecurity.

We have strived to make this work relevant to small companies as well as to large, while recognizing that some of the elements prescribed may be more pertinent to larger companies with a range of integrated systems, functions and processes.

This guide is but one piece of a wider portfolio of work conducted by the World Economic Forum Centre for Cybersecurity and our partners. For example, the *Board Tools and Principles for Advancing Cyber Resilience* published by the World Economic Forum in 2017 set the tone at the strategic level, and executives in smaller organizations may also wish to refer to the Global Cybersecurity Alliance *Toolkit for Small Businesses*.

Looking at the barriers to adoption of cybersecurity best practices, it is apparent that current approaches make it difficult to implement comprehensive best practices across the full extent of the digital and operating environments in organizations. Second, security tools and processes are often set up once and then forgotten, consequently quickly

becoming redundant in a continuously evolving threat landscape. Systems must be updated continuously to keep pace with the flow of business activity if they are to protect effectively against newly discovered vulnerabilities. Third, although organizations have many tools in place to automate security tasks, the tools often can't be used in concert in a fully automated fashion. This results in a complex landscape of security tools, gaps and vulnerabilities and, ultimately, in the inability to deploy a holistic automated approach. Lastly, another major challenge is the sheer volume of work involved in following up on security alerts and incidents that cannot be automated. There is important reliance on humans to carry out security functions, in particular to assess the more strategic implications of alerts and incidents. The shortage of cybersecurity talent, however, means this capability is often under-resourced. To offset these challenges, organizations need to consider outsourcing some of the more advanced, complex and onerous services to service providers, depending on their risk profile, to improve their coverage and service level agreements.

The role of an organization's cyber resilience leaders is to support the mission of their organization by ensuring that cyber risks are managed at an acceptable level. It is unrealistic for any organization to expect that their role is to achieve faultless security, or even that this could be possible. No enterprise is immune to cyber threat and organizations need to assume that a breach will happen. The end goal is resilience, the ability to quickly and efficiently identify and minimize the impact of an incident to allow an organization to continue its mission as effectively as possible.

In the digital age, organizations must continuously adapt their cybersecurity measures in proportion to the growing number and the sophistication of threats they face. According to a survey conducted in 2018 by Willis Towers Watson and the Economist Intelligence Unit (EIU)[2] of 452 large-company board members, C-Suite executives and directors with responsibility for cyber resilience, one-third of the companies surveyed had experienced a major cyber incident that disrupted their operations, and executives cite the size of the financial and reputational risk as the most important reason for board oversight. While about 45% of the North American businesses had confidence in restoration after a breach, this number decreased to 30% for European and only 21% for Asian businesses. To compound this issue, it was reported that on average, only 1.7% of total revenue was spent on cyber resilience.

The following tenets are the fundamentals that an organization must implement in order to embed cybersecurity in the corporate DNA and as part of a comprehensive cybersecurity programme in the exercise of due diligence for cyber resilience. They take into account existing guidance and standards and are intended to serve as a practical guide to cyber resilience for executives when assessing the management of cyber risks in their organization.

10 Tenets for Leaders

Tenet 1

Think Like a Business Leader

Tenet 2

Foster Internal and External Partnerships

Tenet 3

Build and Practice Strong Cyber Hygiene

Tenet 4

Protect Access to Mission-Critical Assets

Tenet 5

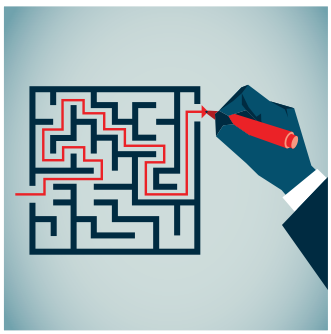
Protect Your Email Domain Against Phishing

Tenet 6

Apply a Zero-Trust Approach to Securing Your Supply Chain

Tenet 7

Prevent, Monitor and Respond to Cyber Threats



Tenet 8

Develop and Practice Comprehensive Crisis Management Plan

Tenet 9

Build a Robust Disaster-Recovery Plan for Cyberattacks

Tenet 10

Create a Culture of Cybersecurity

Tenet 1: Think Like a Business Leader

In the context of the Fourth Industrial Revolution, almost every business is transforming itself by adopting leading technologies and innovative data-driven business models. In this massive, unprecedented wave of digital transformation, cybersecurity operations are a vital element of every business's success. Today a cybersecurity leader's responsibilities include educating the board and the executive leadership on the importance of cyber risk management. While the cybersecurity industry has a tendency to instill fear to sell products, cybersecurity leaders should focus on positioning cybersecurity as an integral component of their business strategy and success.

Over the past decade, the role and significance of cybersecurity within an organization – in general, and that of the cybersecurity leaders in particular – have evolved immensely. Cybersecurity leaders are business leaders, first and foremost, and thus have to position themselves, their teams and operations as business enablers.

Transforming cybersecurity from a support function into a business-enabling function requires a broader view and a stronger communication skill set than was required previously. As an integral part of today's business success, cybersecurity has a direct influence on business reputation, stock value, revenue, brand equity, customer relations and a product's time to market, among other parameters. Consequently, leaders in the digital age must:

- Foster transparency and trust
- Develop the critical thinking, creativity and problem-solving skills not only of the cybersecurity team but of the entire organization
- Possess strong business acumen to translate the technical risks into business strategy risks, so that a non-technical audience can understand the potential threats to business operations
- Understand the business and industry they are in, both to grasp the cyber threats unique to the organization, as well as to use language familiar to the Board and other executives within the organization
- Be proficient in speaking business language when communicating about cybersecurity to influence senior management and the Board of Directors
- Align the objectives of the cybersecurity strategy with the business strategy

The World Economic Forum Centre for Cybersecurity is seeking to change the cyber narrative, which until now has been primarily driven by fear, by highlighting the positive opportunities for building trust in digital transformation.

Tenet 2: Foster Internal and External Partnerships

Cybersecurity is a team sport. By providing vehicles for dialogue and decision-making, internal partnerships enable information security teams to become more agile and responsive to business needs. The number of potential partnerships has grown and will continue to grow as the scope of information risk broadens to include a range of privacy and regulatory concerns as well as traditional security threats. The time to develop such partnership is before a crisis, not after a cybersecurity breach.

Today, information security teams need to partner with many internal groups in their conduct of a variety of functions, including risk management decisions, incident response and monitoring.

A cybersecurity leader needs to develop a shared vision, objectives and KPIs with business executives to ensure that time-to-market timelines are met while delivering a highly secure and usable product to customers in line with the risk tolerance defined by the organization.

The risk tolerance identifies the boundaries of how much risk an entity is prepared to accept. Awareness of residual risk and operating within a risk tolerance provides management with greater assurance that the company remains within its risk appetite. This reassurance, in turn, provides a higher degree of comfort that the company will achieve its strategic objectives.

To ensure that the business in general adheres to legal and regulatory requirements, cybersecurity leaders need to include the legal and privacy executives as key stakeholders in the security journey of the organization.

Such partnerships may include formal structures such as steering committees and risk review boards, as well as informal and ad-hoc entities. Whether formal or informal, internal partnerships are essential to building trust and hence should be created, maintained and managed to purpose, according to organization-specific needs, with a clear definition of involved parties and decision-making authorities.

Beyond building partnerships internally, it is becoming increasingly important to partner with external organizations to share information on security-related issues such as threats and best practices. Sharing security information brings considerable benefits to managing the risks associated with cyber threats or adopting new technologies. This is predicated on trust; the more trusted the relationship, the more sensitive the nature of the information that can be shared.

A key element in fueling information sharing is to increase regulatory protection for victims so as to incentivize the affected parties to share information on cyberattacks and breaches without fear of repercussion. Knowing the key 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.

The World Economic Forum Centre for Cybersecurity convenes public- and private-sector stakeholders in communities of purpose and action to tackle some of the most pressing challenges facing cybersecurity leaders.

Tenet 3: Build and Practice Strong Cyber Hygiene

Effective and consistent implementation of strong cyber hygiene could have potentially mitigated the majority of the cyberattacks of the last decade. Exploitation of known vulnerabilities that exist on a server, application or endpoint device as well as social engineering – understood to mean the psychological manipulation of people into performing actions or divulging confidential information – are leading entry points for a cyberattack, among others. The core security principles that follow are elementary and crucial to building strong security hygiene in an organization:

- **Develop a detailed inventory and configuration management system**

  A clear and thorough understanding of the data supply chain in an organization is critical to building strong cyber hygiene. Organizations must develop and keep up-to-date inventory and configuration management systems that record all enterprise-IT and operational devices, applications and their configuration as well as sensitive data sets in the organization's data supply chain. The systems should include the monitoring capabilities, configuration and status of the devices, data sets and applications.

- **Develop a strong patching strategy**

  Today's businesses run on a heterogeneous infrastructure comprised of numerous components. Any critical system that is out-of-date represents various levels of risk depending upon how it can be exploited and how it is connected to the broader network. Every organization needs to ensure that every component through which any data flows has an up-to-date patching status according to a risk-based assessment of the vulnerability. The patching strategy should include automated scans of the environments for vulnerabilities, automated patch deployments and alerting capabilities. Implementing such a strategy for industrial control systems is a major challenge as legacy systems that have a very long lifecycle may no longer be supported. A renovation plan along with compensating controls will be essential to protecting these critical systems against cyber threats.

- **Implement strong organization-wide authentication**

  Current threat vectors, such as credential stuffing, for instance, abuse weak user credentials and lack of credential challenge mechanisms to fraudulently gain access to user accounts. Multifactor authentication is a proven deterrent and reinforcer of security posture, mitigating cyberattacks that attempt to leverage compromised user credentials. Investment in technologies that enable strong password creation and seamless password management are also proven deterrents. They are highly recommended because they yield high returns for strong cyber hygiene.

  The FIDO Alliance (Fast Identity Online) and World Wide Web Consortium (W3C) have created an open standard enabling the replacement of weak password-based authentication with strong hardware-based authentication to transition to a password-less future.

- **Secure the Active Directory**

  An Active Directory is the core identity platform for many business enterprises and should be considered a critical component in an infrastructure. Companies should start deploying the Microsoft recommended Administrative Tier Model.

- **Enforce data security mechanisms for critical business processes**

  All sensitive data including credentials should be encrypted, at rest and in transit. In the event of a data breach, critical files should only result in obtaining unreadable data. Large amounts of personal information continue leaking into the dark web following data breaches targeting businesses that often fail to implement basic cybersecurity controls such as data encryption and securing of the encryption keys to prevent cybercriminals from accessing and monetizing it.

Tenet 4: Protect Access to Mission-Critical Assets

Investments need to be made to augment or scale identity and access management systems to meet new "perimeter-less" and cloud challenges. Concepts that foster higher business mobility and agility also introduce new complexities into an organization's identity and access management system. Adoption of novel strategy and technologies tailored to an organization's demand is key to safeguarding mission critical assets.

Not all user access is created equal. When defining the roles and policies for every user within an organization, the "principle of least-privileged access" should prevail. For instance, a project engineer does not need access to an organization's financial data and a finance manager does not need to access the organization's production code repository. Building a strong identity and access management system begins with having a single trustworthy reference of all users and their roles within an organization. It is essential to have strong processes and automated systems in place to ensure appropriate access rights approval mechanisms, including for access termination upon an employee's departure or at the end of an engagement with a third party.

For instance, a database administrator within an organization might require access to a data repository to carry out certain functions critical to their job. Robust privileged-user access management is critical in cases of multiple roles across organizations and to avoid toxic combinations. There must be a layered access mechanism for a privileged user to gain access to a mission-critical system. Each layer should be fortified with a different multifactor authentication mechanism based on the sensitivity of the information.

Lastly, comprehensive alert and audit mechanisms should be a mandatory requirement of every identity and access management system. They should be regularly updated based on the new and changing requirements of the organization. These are not meant to be set once and then forgotten. Moreover, a regular review process needs to be adhered to, as projects are completed, and access requirements change.

Tenet 5: Protect Your Email Domain Against Phishing

Email is one of the most valuable and broadly used means of communication, and most organizations strongly depend on it. The internet underlying email protocol (SMTP) was designed almost 40 years ago without security in mind and is susceptible to a wide range of attacks. Email is the most common point of entry, with the median company receiving over 90% of their detected malware via this channel.[3]

Targeted phishing campaigns, in particular, can be more successful by spoofing the originator email address to impersonate a trusted or trustworthy organization or person. This can lead to luring the recipient into giving away credentials or infecting their computer by executing malware delivered through the email. Raising user awareness about how to avoid email fraud is recommended, but insufficient alone – more needs to be done.

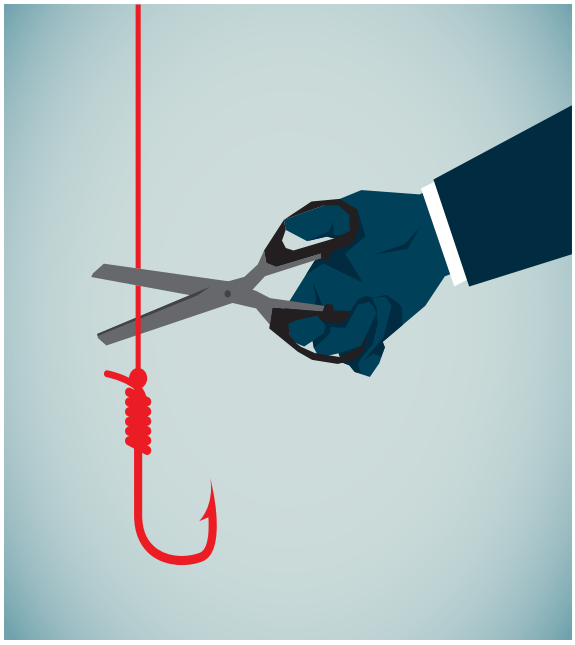
Mitigating the risk of email abuse can be achieved by implementing the following measures:

- Train all employees in recognizing phishing emails, especially senior leadership and departments that handle sensitive information, as they are often the targets of phishing campaigns; this is perhaps the most effective measure to protect your organization against phishing emails
- Stay informed of phishing techniques as new phishing scams are being constantly developed, including by phone ("vishing") and text message ("smishing")
- Implement an email filter to identify and quarantine spam emails, scan hyperlinks and attachments for malicious content and implement specific rules in line with your organization's policies
- Deploy an up-to-date anti-malware software on all endpoint devices as they often come equipped with some type of anti-phishing capabilities
- Adhere to strong cyber-hygiene practices; they will significantly mitigate the risk of a successful compromise through a phishing email
- Implement the free-of-charge Domain-based Message Authentication, Reporting & Conformance (DMARC) standard that helps email senders and receivers work together to better secure emails and to protect users and brands from costly and harmful abuse

Implementing DMARC, in particular, helps to:

- Mitigate the risk to your organization by stopping spear-phishing emails before they reach the users
- Protect other organizations by reducing the risk of their receiving spear-phishing emails that misuse your domains
- Be informed in real-time of new spear-phishing email campaigns, that may put your organization or community at risk

The Global Cybersecurity Alliance provides simple guidelines for how organizations can more easily implement DMARC.



Tenet 6: Apply a Zero-Trust Approach to Securing Your Supply Chain

Nearly 50% of companies fail to assess their hardware and software suppliers' level of cyber risk.[4] As hackers will proactively work to identify and exploit the weakest link in a value chain, a zero-trust approach to securing the supply chain must be the norm.

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 previous versions of their software applications as the demand for new versions is always pressing. To achieve this, the security team needs to adopt novel techniques that enable developers to write secure code from the onset rather than discovering security gaps in the course of code reviews or once in production.

Security-by-design practices must be embedded in the full lifecycle of the project and product development including coding, system architecture, configuration and in the process definition for continuous risks assessment.

Organizations must discard the belief that perimeter security, achievable by firewalls or anti-virus protection, is sufficient. They need adopt a zero-trust approach that does not assume that a company can be made safe and sound within the confines of its own "secure" corporate network. A zero-trust approach places control around the data assets themselves and increases the visibility into how they are used across a digital business ecosystem. Cybersecurity is only as strong as its weakest link.

Following the steps below will help ensure a level of due care for the entire supply chain:

- Limit access in accordance with need
- Conduct due diligence on the backgrounds of vendors with access
- Review the existing contract language; understand the cybersecurity practices of existing vendors
- Contractually bind vendors to security policies and standards
- Audit third-party vendors in accordance with business importance and localization; vendors must be willing to cooperate in maintaining a good enough level of security in line with organizational standards
- Require vendors that process sensitive data to report cyber incidents within 72 hours of occurrence

The World Economic Forum Centre for Cybersecurity is working with the investment community to develop a set of high-level principles and a standard due-diligence framework. This work aims to provide guidance for how investors can not only to evaluate and benchmark their investment portfolio companies and their cybersecurity preparedness, but also influence the new technology being developed in a potential target company by prioritizing security and privacy by design and default. Investor commitment to prioritizing security in new technologies will ensure that the overall attack surface will be reduced by diminishing the number of vulnerabilities.

Tenet 7: Prevent, Monitor and Respond to Cyber Threats

Despite the rising pressure of targeted cyberattacks, with cyber criminals scaling their operations using more sophisticated business models like ransomware-as-a-service and DDoS-for-Hire, and monetizing these efforts through cryptocurrencies, security teams continue to identify nearly two-thirds of all breach attempts on average.[5] However, these occurrences conceal a divergence in performance among organizations. While many organizations are performing well in more mature industries and markets, some are clearly struggling with the increasing pressure of attacks.

New attack vectors and techniques are continuously changing the threat landscape. Detection systems are rapidly outdated if they do not evolve at pace with innovation and should be continuously enhanced by providing inputs from a diverse range of sources. At the same time, novel detection techniques based on machine learning and artificial intelligence technologies should be applied to allow detection systems to be able to ingest this wide variety of data, run regressions and analytics to ultimately produce high-fidelity signals that indicate an anomaly or suspicious activity proactively for further investigation.

Threat intelligence teams should perform proactive hunts throughout the organization's infrastructure as well as keep the detection teams abreast of the latest trends. Organizations must monitor cyber threats both internally and externally, and regularly probe critical and internet facing systems for weaknesses. Moreover, they will need to monitor the internet, social media and the dark web for stolen data and information on key executives and business operations that could be used for social engineering, spear-phishing attacks and scam campaigns. The *Mitre Attack Framework* offers a knowledge base of common tactics and approaches used by adversaries.

The question is not if, but when a significant breach will occur and, therefore, how well a company manages this is inevitability critical.

The key here is to develop a robust risk-based approach to measuring risks and responding to cyberattacks that is tailored to the organization's business context. The security services implemented must be fit for purpose and tailored to the needs of the organization across the following three dimensions:

- The people and organization that will operationalize these services
- The processes and procedures to effectively manage them
- The technologies that will be acquired and implemented

While large organizations can afford to hire in-house cybersecurity experts to manage some complex services (including pen testing, red/blue team exercises, a security operations centre, threat hunting and others), small- and medium-size enterprises should consider outsourcing these services to a managed security service provider, to minimize the hassle and cost in building and training an in-house organization and acquiring the necessary hardware and software. These outsourced services can also often offer better service-level agreements and coverage, which become essential when dealing with criminal organizations that are working around the clock. When considering the outsourcing of security services, businesses need to do their due diligence, engage with reputable and reliable service providers and establish detailed service level agreements.

A three-pronged approach will mitigate the cyber risks in the ever-expanding enterprise ecosystem:

Prevent. Preventive strategies remain as important as ever and must evolve continuously, from their security policies and awareness programmes to the actual access controls they put in place. A multi-layered risk-based approach will fortify the protection of critical assets and minimize the risk of intrusion.

Detect. Prevention is not foolproof owing to the evolving nature of cyber threats, thus having adequate detection mechanisms is essential. Selecting and deploying appropriate controls for the timely detection and notification of compromises is critical. The detective controls must be designed to monitor the critical assets that either store and process sensitive information or are vital for the operations of the organization.

Respond. Detection is rendered pointless without a response. Organizations need to approach cybersecurity in terms of competitive advantage and respond effectively and in a timely manner to a security incident to mitigate the impact to the business, to contain the infected networks and devices and to investigate the source of the attack to determine the vector of infection and patient-zero. The monitoring of the events collected from the various infrastructure and application assets will have to be heightened to track and alert any abnormal activity.

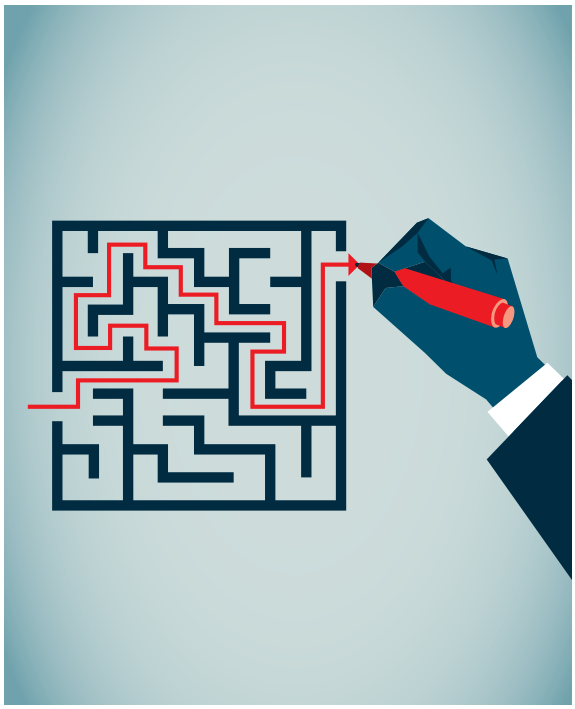
Tenet 8: Develop and Practice a Comprehensive Crisis Management Plan

Crisis management is a critical component of any security programme in today's world, where a security incident is, again, not a matter of if, but when. A typical security organization that focuses solely on analysing and mitigating risk may not be well-positioned to manage a crisis. Thus, building a dedicated team with the aptitude for crisis management is the first building block.

Securing an entire business is an extremely tough job primarily because everything is a priority. Any potential vulnerability could become the next attack point compromising the business. For this reason, many organizations focus primarily on how to prevent and defend while not focusing enough on institutionalizing the playbook of crisis management for the entire organization.

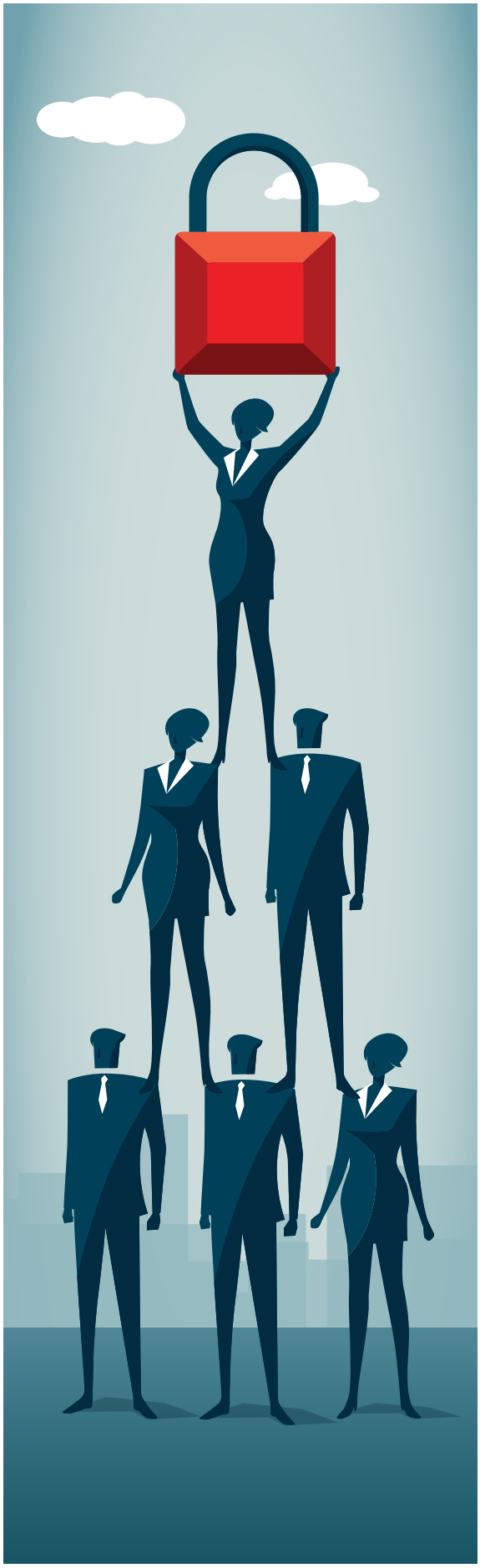
The following aspects are vital to creating a crisis management plan:

- Develop a cross-functional team. The scope of the team ranges from executive leadership and includes the operations, finance, legal, communication, insurance, human resources and technology departments
- When a crisis occurs, a highly detailed plan is invaluable in orchestrating 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 conference rooms that need to be reserved in case of a crisis
- Consider alternative communication paths, including alternate communication mechanisms that do not rely on the core company infrastructure (which might be unavailable during a cyberattack)
- Always keep hard copies of procedures, contacts and other business-critical documentation as a back-up
- Call upon third-party technical, legal and public relations experts, insurance providers during a major crisis to provide unbiased perspectives
- Identify and keep a readily available list of key contacts within law enforcement and applicable regulators, in case of need to communicate with these authorities
- Ensure adherence to global regulatory laws when documenting your crisis management plan
- Focus on the range, motivations and objectives of potential attacks (e.g., espionage, denial of service, financial gains, etc.).
- Practice regular tabletop exercises and simulations to ensure readiness in the event of a crisis
- If the organization doesn't communicate, others will, and many "experts" will be happy to speculate
- Consider that occurrence of breaches may be particularly heightened during business downtime and retain vigilance during these periods (e.g. outside office hours, during the holiday season)
- Avoid over-reliance on technology to support your plan; systems and communications may not be available during a cyber incident



Timeliness is as important as transparency and simplicity to form a solid trusted relationship with customers, shareholders, regulators and other stakeholders. In the recent past, there have been numerous nefarious examples of companies that have failed to communicate a security incident to their customers or communicated only when required by a regulatory body. In certain cases, such as the Yahoo data breach in 2016, delayed communication of an incident allows attackers to misuse compromised customer data even before the customer is notified. In contrast, the Norsk Hydro cyberattack that hit the aluminum manufacturing giant in March 2019 highlighted the benefits of a perfectly orchestrated incident response and communication plan which resulted in higher stock prices. These serve as good examples for ensuring the timeliness of security incident communications.

In the event of a security incident, it is important to notify to customers is that the tenure is limited to the incident and not the potential aftermath for the victims of the incident. Organizations often communicate publicly with their customers about a potential compromise of data without acknowledging that such communication is an opportunity for cyber attackers to mislead their customers. Quite often a wave of sophisticated phishing attacks is launched targeting customers of a business that have recently reported a security breach. News of a breach often requires customers to take certain action such as, for example, providing information to check whether they were affected by the incident.



Tenet 9: Build a Robust Disaster Recovery Plan for Cyberattacks

As society becomes more reliant on technology and cyberattacks proliferate, it is vital that all organizations, regardless of their size, be prepared for the worst. A major breach of mission-critical assets can have disastrous reputational, operational and financial impact on an organization that fails to take extensive measures to protect itself.

Fires, storms, blackouts and other physical events are all unpredictable, yet their nature is generally well understood. Security threats, on the other hand, are both unpredictable and, given the rapidly advancing nature of cyber criminality, not generally well understood. This means that security recovery strategies must be revisited and updated even more frequently than disaster recovery strategies. Furthermore, cybersecurity leaders need to be integral elements of the disaster recovery team and be consulted before a disaster is invoked as a result of a cyberattack.

A disaster recovery and continuity plan must be tailored to security incident scenarios to protect an organization from potential cyberattacks and to instruct how to react in case of a data breach. Furthermore, it can reduce the amount of time it takes to identify breaches and restore critical services for the business.

Follow these best practices when developing your plan:

- **Define your key assets**

  To successfully defend your company against attack, you must first know what you're protecting. What are the key assets that would cause loss to your company and your stakeholders if hacked? Convene your management team to discuss such potential losses and how to mitigate such threat

- **Identify recovery solutions**

  After defining your company's most important assets, the next step is to determine the means of recovery in case of data breach and cyberattack. The recovery plans or mitigation plans allow the company to continue at acceptable levels. For example, they may include saving data to a backup disk, server or cloud storage – or perhaps a complete data replication to a secure offsite location

- **Develop and communicate the governance**

  In the case of an emergency, it's important to know who is responsible for officially declaring a disaster and enacting a communication chain.

- **Review and practice your plan regularly**

  For your plan to perform effectively as designed, it is important that you review it with employees regularly, so everyone understands what to do when faced with a data breach or major cyberattack. Be sure to update the plan in line with new policies added and personnel changes, and secure practice by means of tabletop exercises and simulations.[6]

In addition to a disaster recovery and continuity plan, you may want to consider cyber insurance. While the overall cost of data breach detection is increasing as cyberattacks become more sophisticated, cyber liability insurance helps lower these costs.

Tenet 10: Create a Culture of Cybersecurity

The traditional enterprise security paradigm, often expressed in castle-and-moat terms, described a technology boundary that isolated and protected the workers behind it. Today, however, a growing number of user interactions with the outside world bypass the physical and network perimeters and the security controls they offer. They take place on external websites and social networks, on laptops in coffee shops and homes, and continuously on personal devices such as smartphones and smartwatches.

This changing environment doesn't mean that the security perimeter has disappeared. Instead, it has shifted to the users and their multiple endpoints. As a result, identity has become the new perimeter. Every day, users make decisions that can have as much impact on security as the technical controls we use.

Keeping an organization secure is every employee's job: front-door attack vectors such as phishing, for example, are leveraged by many attackers. This puts users in the first line of defense and recognizes the critical role all employees play in the organization's security. It is important that the security rules and the technology provided enable users to perform their job as well as help keep the organization secure. According to the IBM X-Force research in 2018, 43% of compromised records were linked to human error and misconfigured IT services,[7] and 75% of these incidents involved malicious intent, with negligence accounting for the remainder. Thus, organizations should be mindful of the fact that a majority of data breaches are perpetrated by internal actors. This can occur through unintentionally disclosing sensitive information, clicking on a phishing link, the negligent use of unsecure USB drives, WIFI networks, use of weak or reused passwords, or bad password sharing practices.

The following practices will help foster a stronger culture of cybersecurity:

- Develop user awareness and training tailored to the business context and different user groups across the organization.
- Implement a streamlined delivery of awareness campaigns by leveraging diverse and novel ways for better engagement and penetration across the organization.
- Incentivize your employees for participating in the awareness campaign and reporting suspicious activity. For instance, the Aviation industry has consistently maintained very high safety standards by implementing effective training and awareness programmes to sensitize all employees to report any incidents and then investigate them. A similar approach should be taken for cybersecurity incidents.
- Enforce sanctions on major or repeat offenders in line with the organization's code of conduct

Elementary security knowledge should become mainstream and organizations should partner with academia and government educational systems to develop a curriculum that is adapted to the actual needs of their industry to develop a cybersecurity workforce equipped with the skills needed in the digital age.

The World Economic Forum Centre for Cybersecurity is working with its partners to address the cybersecurity skills gap, through working with global leaders to find scalable ways to tackle the shortage of cybersecurity skills and help countries with nascent digital economies jump-start their tech sector.

Conclusion

Troels Oerting
Chairman of the Advisory Board
Centre for Cybersecurity
World Economic Forum

Today's cybersecurity leaders are a different breed from those of the past. The nature of the role has rapidly changed from a technology-oriented position to a business leadership responsibility, and the evolution is far from over.

A successful cybersecurity strategy and its implementation are dependent on the culture of the organization. Cybersecurity, privacy and digital trust are all based on how well the organization manages to integrate security as an inherent part of its DNA.

The importance of fostering an environment of security and risk awareness, shared ownership of cyber risk and cyber risk resilience is only going to grow. Cybersecurity leaders who are able to step beyond a tactical, technical level are more likely to gain credibility and support among leaders across the enterprise, including the board, C-suite, and business unit leaders.

In the Fourth Industrial Revolution, all businesses are undergoing transformative digitalization of their industries that will give access to new markets, as well as a hope of a better and more prosperous world.

This digital transformation is powered by disruptive technological advancements such as 5G, AI, Cloud computing and the connection of the physical world to the digital through IoT technologies, which will connect everything, generate petabytes of data and increase the attack surface and number of attack vectors.

This explosion of connectivity provides companies with tremendous opportunities to increase operational efficiencies, improve customer satisfaction and experience. It comes with a caveat, however: As customer data, intellectual property and brand equity evolve, they become new targets for theft, directly impacting shareholder value and business performance. In response, business leaders need cybersecurity leaders to take a stronger and more strategic leadership role. Inherent to this new role is the imperative to move beyond the role of compliance monitors and enforcers to better integrate with the business, manage information risks more strategically, and work toward a culture of shared cyber-risk ownership across the enterprise.

When assessing cyber risks, cybersecurity leaders are now called upon to assess the business impact and have metrics to measure the operational, regulatory compliance and financial impact. Like in the physical world, perfect security does not exist in the digital world and trade-offs must be made. Businesses and key stakeholders need to make better informed decisions on the risk appetite of their organization to define a good enough cybersecurity posture. This would entail assessing the threat landscape, the attackers' motives and tactics as well as identifying critical digital assets, known vulnerabilities to prioritize the appropriate level of controls required with regard to people, processes and technologies.

Strong cybersecurity has become fundamental to a resilient business and industry ecosystem. With effective cyber-risk management, businesses can achieve smarter, faster and more connected futures, driving business growth. 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.

Contributors

The World Economic Forum would like to like to thank the following partners and contributors to this publication:

Kelly Bissel	Senior Managing Director, Accenture Security, Accenture, USA
Craig Froelich	Chief Information Security Officer, Bank of America, USA
Paul Gillen	Managing Director, Head of Security Operations and Deputy Chief Security Officer, Barclays, UK
Rob Wainwright	Senior Partner, Deloitte, Netherlands
Rosa Kariger	Global Chief Information Security Officer, Iberdrola, Spain
Jim Alkove	Executive Vice-President, Security, Salesforce, USA
Anthony Dagostino	Global Head of Cyber Risk (2016-2019), Willis Towers Watson, USA
Peter Foster	Chairman of Global FINEX Cyber and Cyber Risk Solutions, Willis Towers Watson, USA
Paige Adams	Group Chief Information Security Officer, Zurich Insurance Group, USA

From the World Economic Forum

Georges de Moura	Head of Industry Solutions, Centre for Cybersecurity; Lead Author
Troels Oerting	Chairman of the Advisory Board, Centre for Cybersecurity

The Forum also wishes to acknowledge the contribution of Algirde Pipikaite and Amy Jordan, Project Leads, at the Centre for Cybersecurity.

Endnotes

1. Zurich Insurance Group note. Mitigating cyber risk could make a difference of $120 trillion to global economy by 2030. https://www.zurich.com/en/media/news-releases/2015/2015-0910-01 (link as of 23/10/19)
2. Infographic: Global insights on cyber-intrusions and organizational confidence https://www.willistowerswatson.com/en-BE/Insights/2018/07/infographic-global-insights-on-cyber-intrusions-and-organisational-confidence (link as of 23/10/19)
3. 2019 Verizon Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/dbir/ (link as of 23/10/19)
4. Global Cyber Risk Perception Survey. https://www.marsh.com/us/insights/research/global-cyber-risk-perception-survey.html (link as of 23/10/19)
5. 2018 State of Cyber Resilience report. https://www.accenture.com/pl-en/insights/security/2018-state-of-cyber-resilience-index (link as of 23/10/19)
6. Healthcare Business and Technology. https://www.healthcarebusinesstech.com/cyber-attacks-recovery-plan/ (link as of 23/10/19)
7. IBM 2018 Cyber Security Intelligence Index. https://www.ibm.com/security/data-breach/threat-intelligence (link as of 23/10/19)

WORLD ECONOMIC FORUM

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