WORLD ECONOMIC FORUM

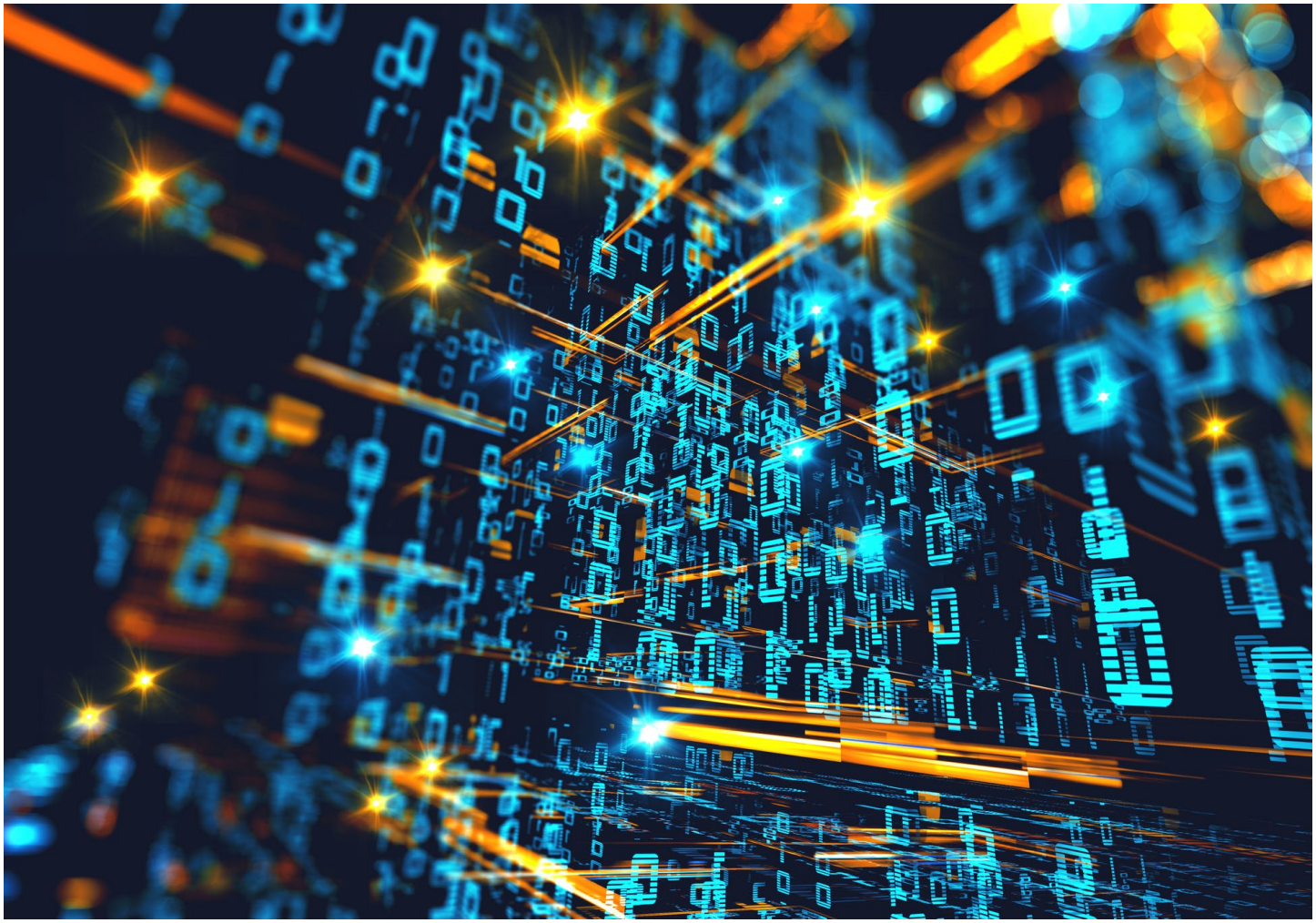
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust

Incentivizing Responsible and Secure Innovation

A framework for investors and entrepreneurs

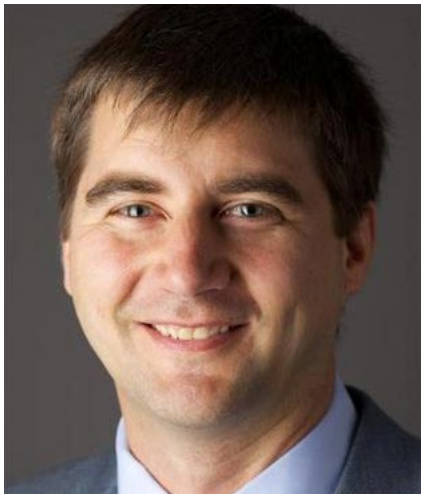
June 2020



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

Preface



Jeremy Jurgens
Managing Director
World Economic Forum

Technological disruption is one of the most daunting challenges of the 21st century. Technology and innovation bring many positive changes and opportunities but if they are not developed with security in mind, they present more risks and potential disruption than provide solutions. In recent years, private- and public-sector leaders have become increasingly aware of the existential dimensions that cyber risk presents. According to the World Economic Forum *Global Risks Report 2020*, cyberattacks are ranked the second risk of greatest concern for business globally over the next 10 years.[1] Cyberattacks on critical infrastructure – rated the fifth top risk in 2020 by the expert network – are becoming even more prominent in sectors like energy, healthcare and transportation. The COVID-19 pandemic and resulting dependency on technology is underscoring the crucial importance of cybersecurity more than ever. The *COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications* released by the World Economic Forum in May 2020 reports that an increase in cyberattacks and data fraud is the third most worrisome fallout for companies for over 50% of executives surveyed and the breakdown of information technology infrastructure and networks is a top concern for companies according to nearly 30% of respondents.[2]

Digital technologies are introducing new vulnerabilities faster than they can be secured and the prospect of curbing cyberattacks diminishes with each additional unsecured technology. Technologies are at increased risk because cyberattacks could cause more traditional, kinetic impacts as technology is being extended into the physical world, creating a cyber-physical system.[3] Nevertheless, applying principles such as privacy-by-design and security-by-design and integrating cybersecurity features into new products are still only a secondary concern to getting products to market as quickly as possible.

There is an imbalance between the time to market and time to security. Market forces pressure for shiny new products and tech gadgets or applications, they care little about the security embedded in a new technology. This trend rewards entrepreneurs who develop new products as fast as possible and market them at the earliest availability, disregarding that this creates an enormous attack surface of ever newer products filled with vulnerabilities for cyber criminals to exploit. Were entrepreneurs and innovators encouraged and incentivized to prioritize security features in their product development from the very beginning, a much safer cyber space would be incrementally possible. Consumer behaviour is changing and consumer concerns about privacy and security are growing[4], inevitably leading to changes in market forces. But these changes are not occurring fast enough.

The purpose of this insight report is to provide tools and guidance for entrepreneurs, innovators and investors to enable them to improve security features in new technologies and incorporate cybersecurity features from the get-go. We present here a number of essential cybersecurity requirements to be considered when developing new technology, innovation and new companies, to ensure their resilience. In addition to the cyber essentials, the report provides a conceptual framework and guidelines for cyber-risk assessment specifically designed for entrepreneurs and investors. This assessment process involves analysing cyber-risk exposure, taking stock of cybersecurity preparedness capabilities, understanding the cyber culture in an organization and its readiness to respond to cyber incidents.

Readers will find a detailed description of each cyber essential followed by practical steps for entrepreneurs on their implementation and guidance for investors on how to validate them. It is important to emphasize that cyber essentials will need to be tailored to each organization, based on its size, nature and type of product.

The World Economic Forum seeks to help smaller organizations understand how they need to develop their cybersecurity capabilities and build a cybersecurity strategy from the very early stages of their operations, tailored specifically to the organization's needs.

Our key message is that a cybersecurity focused culture is, or should be, the starting point of any development, supported by security-by-design and privacy-by-design principles and practices, and guided by a roadmap for the continuing development of cybersecurity requirements (e.g. governance, resilience), in line with an organization's growth. Our goal is to raise awareness and provide a practical framework for entrepreneurs and investors so they can incorporate cybersecurity in their strategic decisions, make cybersecurity an integral part of their corporate growth strategy and consider cybersecurity as a business enabler.

Foreword

Martina Cheung
President
S&P Global Market Intelligence
USA

Our work with the World Economic Forum focuses on developing guidance and tools for business leaders and investors to build a more secure future by giving serious attention to and putting responsible emphasis on cybersecurity when we innovate and create new technologies.

Every single business and industry is impacted by digitalization. Klaus Schwab, founder of the World Economic Forum, coined this shift as the Fourth Industrial Revolution: an era that builds and extends the impact of digitalization, and introduces entirely new ways in which technology becomes embedded within societies.[5] Organizations are taking advantage of digitalization and developing entirely new ways of communicating with customers, partners and staff to improve business processes and develop new products through a digital supply chain. The COVID-19 pandemic in early 2020 has resulted in millions of businesses around the world relying solely on digital tools as the means of communication among their employees and clients. 451 Research, an S&P Global company, surveyed over 800 information technology decision-makers and found that fewer than 20% are spending more money on information security due to the coronavirus outbreak[6], potentially leaving other businesses open to security gaps.

As dependency on technology and digital solutions grows exponentially, 68% of business leaders acknowledge their cybersecurity risks are also on the rise.[7] Nearly 80% of organizations are introducing digitally fuelled innovation faster than they can secure it against cyberattackers.[8] The nature of digital technologies makes them intrinsically vulnerable to cyberattacks that can take a multitude of forms – from data theft and ransomware to the overtaking of systems with potentially large-scale harmful consequences.[9]

Since the beginning of the internet, digital tools and technologies were developed with convenience and speed in performance being top of mind, while security was a secondary concern. The introduction of innovation and the Internet of Things (IoTs) is drastically increasing the potential cyberattack surface. For example, it is estimated that there are already over 21 billion IoT devices worldwide[10], and their number will double by 2025.[11] Attacks on IoT devices increased by more than 300% in the first half of 2019.[12] These actions were not just to attack an endpoint, but to access the full network and use the IoT device maliciously. With the additional employees, clients, suppliers and others now working remotely due to COVID-19, many of those unprotected endpoints are cause for concern for information security professionals.

Organizations that experience cybersecurity incidents are likely to incur substantial costs like remediation, repairs of systems and legal costs. In some extreme cases, the consequences

can also include regulatory actions by national, state and federal government authorities, as well as reputational damage that adversely impacts customer or investor confidence. All these consequences could damage a company's competitiveness, stock price and long-term value. According to an IBM security report, the average cost of a data breach in 2019 was $4 million and it takes around 279 days to identify and contain a breach in an organization. IBM also found that two-thirds of the resulting costs tend to occur in the first year after the breach.[13]

As digitalization spreads across the global economy and within businesses, we typically focus on incidents of significant impact, on larger organizations covered by the media, or businesses where regulators require certain levels of disclosure. We should not forget, however, that entrepreneurs are typically small and medium-sized enterprises (SME) and that SMEs represent about 90% of businesses and more than 50% of employment worldwide.[14] Cyber-related incidents could have a dramatic impact on their survival.

The goal of providing cyber essentials in this report is to advance cybersecurity culture and awareness among entrepreneurs, innovators and investors, and to encourage public and private collaboration to continue building innovation ecosystems with security in mind. This report is intended for decision-makers and investors in large enterprises but also in small and medium-sized businesses. With these practical guidelines, we hope that the market will succeed in ensuring that innovation is secure, responsible and – most important of all – trustworthy.

Society is increasingly dependent on digital technologies, and these technologies increasingly affect the world in a direct physical manner. A robust and resilient cybersecurity requires two things: a holistic approach to the problem and diversity among those proposing solutions. Everyone needs to step up: users and consumers, governments and regulators, corporations and investors. A successful future of our digital economies depends on integration of cybersecurity principles like privacy and security by design from the get-go of technology development. These practical steps and best practices proposed by the World Economic Forum will help companies incorporate security into their new products from the beginning

Bruce Schneier
Lecturer
Harvard Kennedy School of Government
USA

1. Introduction

This is the second report in a series of insights and resources published in the framework of the World Economic Forum initiative on Incentivizing Secure and Responsible Innovation, conducted by the Platform for Shaping the Future of Cybersecurity and Digital Trust. Following a first report proposing a cybersecurity due diligence framework for the investment community, this edition focuses on practical guidance to a broader community involved in developing technological innovation, including entrepreneurs and investors.

Resilience in cybersecurity can be achieved only by involving different stakeholders and influencers in ensuring that the entire innovation and technological ecosystem is aware of the benefits of robust cybersecurity. A serious change in mindset is needed to realize that cybersecurity is a business enabler that supports agility, improves innovation and ensures stable growth. Leading technology companies agree that cybersecurity is becoming a competitive differentiator among technology developers and platform providers as consumer concern grows about the implications of technological development for privacy and security.

This report contains three sections to help guide entrepreneurs and investors on cybersecurity:

Incorporating cyber essentials into the business life cycle

This section focuses on how to implement cyber essentials into business processes. Entrepreneurs must understand the importance of cybersecurity when launching new products, innovating and developing new entities. Investors, on the other hand, should have the tools to evaluate the state of cyber preparedness of their potential investments. The cyber essentials proposed here were developed by a community of stakeholders including executives from technology companies, investment firms, credit rating agencies, entrepreneurs, academics and public policy experts. Their purpose is to enable entrepreneurs to both assess and develop the cybersecurity capabilities of their companies and products. It is important to note that entrepreneurs need to effectively tailor their commitment to cybersecurity, based on their organization's level of resources, talent, size and maturity level.

The second part of the report is written for two focus groups: entrepreneurs and investors.

Cyber essentials and practical guidelines for entrepreneurs

Cyber essentials are presented in three distinct security categories: organizational, product and infrastructure, followed by their explanation and practical implementation guidelines for entrepreneurs. It is vital that entrepreneurs apply and develop their cybersecurity capabilities continuously based on the degree of maturity of their enterprise and product development lifecycle. The practical guidelines are designed to facilitate implementation of each cyber essential.

Cyber essentials and practical guidelines for investors

Each cyber essential description is followed by practical guidelines enabling investors to verify and validate their target investment. The checklist of cyber essentials provides tools for investors to conduct a robust due diligence assessment of the cybersecurity capabilities of potential investments. The practical validation guidelines for each cyber essential provide the most important questions investors need to ask to accurately evaluate their investment target. Gathering the suggested data will inform the investment decision.

2. Incorporating Cyber Essentials in the Business Life Cycle

In the building of innovative business models and technology solutions, cybersecurity is essential to protect data, intellectual property, online transactions and to ensure user trust. Cybersecurity is an enabler of the everyday operations of most businesses today and its significance will only grow in the future. In terms of successful business conditions, cybersecurity is a business management challenge that requires a strategic and unified approach across all business units.

Cyber essentials application throughout the business life cycle

Executives have a decision to make: What is the significance of cybersecurity in their organization? They can choose either to commit to cybersecurity and strive to apply best practices by implementing cybersecurity essentials to ensure the longevity of business operations, or they can treat cybersecurity as a mere compliance requirement. We maintain that it is vital for the founders and investors of a new business to commit to cybersecurity if they are to succeed in building cyber capabilities and foster a cyber-focused environment. A commitment to cybersecurity implicates awareness and ensures the initial allocation of resources to prioritize cybersecurity in corporate and product development. It is equally important to develop a cybersecurity strategy for all business units and incorporate it as an integral part of business strategy. A well-developed cyber strategy helps to guarantee that the cyber essentials are applied throughout the business life cycle from start-up stage to maturity. Early commitment to cybersecurity allows executives to ensure that they have a strategy to secure the potential attack surface of their enterprise comprising all systems, networks and third-party exposure.

Cyber awareness is important to all companies regardless of size and stage of development. An organization needs to incorporate the

cyber essentials into their business processes, technology application and employee awareness. The cyber essentials chart a path to cybersecurity beyond compliance to focus on cyber resilience and preparedness.

Adherence to cyber essentials should be reviewed and assessed regularly by company leadership to understand and evaluate the company's security performance. Executive leadership should ensure that any gaps and areas for improvement detected are in fact addressed in a broad set of solutions in cybersecurity governance, privacy- and security-by-design.

Cybersecurity is a constantly evolving, dynamic process calling for regular assessment of risk and consideration of all the parameters that could reduce risk to acceptable levels in accordance with changing business needs and challenges. It cannot be emphasized enough that as the types of attacks continuously evolve and the corporate digital footprint changes on a virtually daily basis, cybersecurity must be adapted and updated at regular intervals.

Incorporating cyber essentials in business processes and corporate culture must be an ongoing process, not a once-a-year audit or compliance effort. The commitment to prioritize cybersecurity rather than considering it as an afterthought must be firmly rooted in and throughout the corporate culture, and the product and services development cycle. A detailed cybersecurity programme and strategy does not have an end goal, but rather is an ongoing process that must be adapted and adjusted on regular basis.

> *"Cybersecurity is a business enabler of everyday operations of today's businesses and will increase in significance in the future. These cyber essentials present the most important requirements that will provide a robust cybersecurity framework for entrepreneurs and innovators. Businesses that prioritize cybersecurity in their strategy will thrive in the future."*
>
> **Haiyan Song**
> Senior Vice President and General Manager
> Security Markets
> Splunk, USA

2.1 Commitment – The entrepreneur's responsibility

When developing a new technology or company, entrepreneurs have multiple competing interests and priorities to ensure they build a good product or service and a sustainable business. Due to these multiple competing interest areas, cybersecurity does not necessarily get the attention and resources it warrants. Today there is virtually no industry or sector immune to cyberattacks. Irrespective of the size of the company or its industry, the vulnerable, weak points are often exploited by hackers and cyber criminals. Entrepreneurs have a responsibility to ensure that their companies and products are secured digitally and that they have a recovery plan ready to activate should hackers succeed. This is more important for small and medium-sized enterprises, to which a cybersecurity incident could be fatal or diminish its valuation and attractiveness for investment.

With more than 1 million new consumers connecting to the internet each day, cybersecurity is becoming an important enabler in building consumer trust and ensuring business sustainability. Entrepreneurs and innovators who prioritize cybersecurity have an opportunity to differentiate their company and product in the field. Cybersecurity is a business enabler, but only on the condition that it is supported by strategic investment in company culture, staff and technology.[15] The cost of actions not taken, products not created, and markets not entered into because of unmanaged cyber risk outweigh the investment needed to ensure cyber resilience and preparedness. Entrepreneurs need to hold their companies to a standard in which cybersecurity and innovation fully complement one another. This means increasing everyone's focus on positive cybersecurity impact and its role in safeguarding business processes, intellectual property and sensitive data. Cultural change that integrates cybersecurity into product development processes and considers everyone in the firm's ecosystem as responsible partners is an opportunity to enhance trust.[16]

The rapid growth of cybercrime in recent years is a worrying trend. Regulators around the globe are introducing legal measures – such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, the Brazilian General Data Protection Law (LGPD)[17] – to ensure that organizations prioritize cybersecurity, privacy and resilience. Future incidents of data loss will add significant cost in addition to the financial impact of attacks as regulators start to impose fines.

Features such as security-by-design are highly important for product development because as a system develops, it becomes harder and more costly to add security measures. The practice of security-by-design is becoming crucial in our rapidly evolving world in which hyperconnectivity is increasingly connecting everything and changing the way we live, work, travel, communicate and spend our leisure time. And while connecting everything through IoT and 5G technology offers a wide range of opportunities for manufacturers, developers and consumers, the vast connectivity at 5G speed poses major security risks. As greater numbers of devices are interconnected, securing them all is the biggest challenge. Hardware, software and connectivity will all need to be secure if IoT devices and 5G are to work effectively.[18] Without security, any connected object, from a vehicle to a medical device, can be hacked. Once hackers gain control, they can take over the object's functionality, steal the user's digital data and access the network that the IoT device is connected to.

> *"As digital devices move into our homes, offices, hospitals and cities, they are providing a venue for attackers to enter our networks. It is important to keep that in mind when designing new networked devices and incorporate cybersecurity features in every stage of product development, but the real focus and challenge is to prioritize cybersecurity from the get-go. The earlier that cyber essentials are incorporated in the product, the cheaper it is to sustain security and durability at later stages."*
>
> **David Li**
> Executive Director
> Shenzhen Open Innovation Lab (SZOIL)
> People's Republic of China

2.2 Strategy – Enabling investors to validate cyber essentials

Investors need to grasp that security is a smart investment, not an unnecessary cost.[19] Investors who provide capital to start-ups and small and medium-sized companies that develop technology innovation must guide them to better cybersecurity within their target companies and in technology development. A cyber-risk assessment is crucial to any organization's risk management strategy. It provides an informed overview of an organization's cybersecurity posture and provides data for cybersecurity-related decisions. A well-managed assessment process prevents costly waste of time, effort and resources and enables informed decision-making.

The due diligence process must adapt to manage the risks of new kind s of investments and acquisitions. An investor's failure to identify potential problems early on can lead to liabilities down the road. Recent research by Forescout Technologies found that 53% of information technology and business decision-makers reported that their organizations uncovered a material cybersecurity incident that put a potential merger or acquisition deal at risk.[20] As society becomes more dependent on technology and data-driven decisions, cybersecurity ought to be woven into every business and investment decision.[21] As a result, the fiduciary duty for investors increasingly involves assessing the cyber risk of their target investments, monitoring and mitigating the cyber risk of portfolio companies.[22]

This report provides investors with practical tools with which to confidently assess cyber risk with the same rigour as any other risks they analyse and manage. Cyber due diligence is becoming part of the broader due diligence process and this report provides investors with the tools to verify their target company's cyber preparedness and resilience in practice, developed on the basis of the first publication in this series, released in 2019: Incentivizing Responsible and Secure Innovation: Principles and guidance for investors.

3. Application – Recommended Cyber Essentials

The cyber essentials developed by the World Economic Forum and its partners consist of core cybersecurity principles and requirements to be applied when developing new companies and innovation. These cyber essentials represent what we consider to be the most important requirements that, if implemented, will provide a robust cybersecurity framework encompassing organizational, product and infrastructure security.

Cyber essentials encompassing organizational, product and infrastructure security

3.1 Organizational security

Cybersecurity culture

An effective cybersecurity culture should clearly state the critical nature of cybersecurity in company practice and every employee must understand their role and responsibility to act in a secure manner to keep company assets and the network safe, upgrade their knowledge through regular training and actively foster habits that enhance a security culture.

Entrepreneurs: When setting up a new entity and defining the principles that guide company culture, the entrepreneur should incorporate cybersecurity hygiene and nurture cybersecurity principles into the organization's overall corporate culture.

Investors: When assessing the culture of a target company, investors should evaluate whether the cybersecurity culture is part and parcel of the overall corporate culture.

Cybersecurity governance

Cybersecurity governance is a subset of a corporate governance that provides a strategic direction for cybersecurity activities and oversight of cyber risk in an organization. Cybersecurity governance is the means by which organizations control and direct their approach to security.

Entrepreneurs: As entrepreneurs set up their entity's business procedures, cybersecurity governance must be incorporated therein.

Investors: When assessing the health of a target's corporate governance structure, investors must ensure that cybersecurity governance is incorporated therein.

Cyber resilience

Cyber resilience refers to an entity's ability to continuously deliver the expected services and operations despite adverse cyber events. Cyber resilience also refers to organization's ability to observe its networks and digital footprint to gauge how quickly it can respond to any occurring changes. It measures how well an organization can continue operating regardless of cyberattacks, technical failures and other significant cyber disruptions of normal business processes.

Entrepreneurs: When setting up a new entity, entrepreneurs should integrate cyber resilience into their corporate operational resilience and business continuity risk management.

Investors: When assessing corporate resilience and business continuity, investors should evaluate whether cyber resilience has been incorporated into the target's overall corporate resilience.

3.2 Product security

Security-by-design

A security-by-design approach to product development includes security features as a fundamental component, capable of reducing the number of vulnerabilities and diminishing the attack surface throughout the development process.

Entrepreneurs: When developing a new product or system, entrepreneurs must incorporate security-by-design into the product development life cycle and empower their security development teams.

Investors: When evaluating a target company and their product(s), investors should validate whether security features are part of the design criteria and security-by-design principles are adhered to throughout the product development life cycle.

Privacy-by-design

Privacy-by-design refers to the prioritization of data protection throughout the entire engineering process. By applying the privacy-by-design principle, the software and systems are designed with privacy features as priority, a comprehensive understanding of what could be done with the collected data and what actions should be avoided.

Entrepreneurs: When developing a product, entrepreneurs must establish privacy as a foundational tenet of the product development life cycle and embed this as such in every step of the product development and product maintenance process.

Investors: When assessing a target company in which they want to invest or acquire, investors should verify the privacy policy of the target company and confirm that the privacy-by-design principle is incorporated in the product development life cycle

3.3 Infrastructure security

Data governance

Data governance manages the confidentiality, integrity and availability of the data in enterprise systems, through internal data policies and controls of data use. Effective data governance ensures that data is consistent and trustworthy.

Entrepreneurs: In building an enterprise, it is important to develop and maintain a data protection policy, including a written and comprehensive information security programme to ensure the confidentiality, integrity and availability of personal and enterprise data held.

Investors: When assessing a target, it is important to verify if they have a data governance and protection policy compliant to the required industry-specific, national, and international regulations.

Third-party security

Third-party security focuses on protecting an organization against cybersecurity threats that could originate from the supply chain, vendors or customers.

Entrepreneurs: As part of developing an enterprise, entrepreneurs need to understand and manage potential third-party risks by mapping out their third parties and developing a third-party risk management framework.

Investors: When assessing a target company, it is important to understand their third parties, and the supply chain and other risks associated with them.

> *Too often, cybersecurity is viewed only as an information technology (IT) issue that only IT professionals are responsible for. The cyber essentials framework reframes cybersecurity into a strategic business challenge transcending across organizational, product and governance issues for all entrepreneurs, innovators and their investors.*

Pascal Millaire
Chief Executive Officer
CyberCube
USA

4. Assessment of Cyber Essentials

4.1 Cybersecurity culture

People are the most important asset of any well-developed and implemented cybersecurity programme. One meaningful way to increase cybersecurity awareness is by training all personnel, from board members to developers, according and adapted to their roles and responsibilities. It is common to underestimate the damage that could potentially be caused by personnel and to overestimate technology's ability to limit such incidents. According to a PWC study, just 27% of corporate executives believe their board receives adequate metrics for cyber and privacy risk management.[23] This percentage is alarming, showing as it does that not enough board members are informed or have the right tools to consider and manage cyber risk and, consequently, are ill-equipped foster a cybersecurity culture.

A cybersecurity-focused culture based on cyber expertise and awareness is vital to effective cybersecurity and resilience. Successfully defending against cyberattacks requires a coordinated effort across all levels of a business, reinforced by conscious recognition that cybersecurity is a genuine business enabler, not just a cost centre. As most businesses, investment targets and their key assets are either becoming digital or are already in the digital domain, it is important to foster a cybersecurity awareness culture in today's digital workplace. In many organizations, across a wide range of industries, key customer data or intellectual property may be accessed by employees on an almost daily basis. Fighting cybercrime and staying alert should be an enterprise-wide concern and employees play the most important role in this. According to research conducted by the UK Information Commissioner's Office (ICO), 90% of data breaches are caused by human error.[24] Essentially, a cybersecurity culture in the workplace ensures seamless integration of safe cybersecurity practices in the work of its employees.

A cybersecurity culture, should be fostered across all business units of an enterprise. No single leader or team can grasp the full perspective needed to be effective in the cyber domain. No one group within an organization can manage the number and types of internal and external threats, the complex technological landscape and the many actions needed to address vulnerabilities associated with people and technology. It is much more effective to work together, with every employee understanding their role and responsibilities in protecting the organization. An effective cybersecurity culture empowers employees to raise their cybersecurity-related concerns, whether signalling poor practices like weak passwords or highlighting technical vulnerabilities. Part of this empowerment includes employee understanding of their endpoints, receiving regular training and actively fostering habits that enhance security culture. To examine culture in the context of cybersecurity requires delving into the personal beliefs, unconscious biases and habits that inform these security-related behaviours across the enterprise.

According to a recent survey by the Information Systems Audit and Control Association (ISACA), 95% of global respondents identify a gap between their current and their desired organizational cybersecurity culture, and agree there is much progress to be made.[25] A significant 33% of surveyed executives acknowledge a substantial gap. These firms have yet to experience how a strong cybersecurity culture will impact operations, create brand loyalty and a competitive advantage in the marketplace.

The main differentiator of organizations that have achieved their desired cybersecurity culture is that they have a cohesive management plan and the commitment of leadership to focus on cybersecurity. Managing a successful cybersecurity culture requires a leader and a plan, yet only 58% of organizations have outlined a cybersecurity culture management plan or policy.[26]

What does **cybersecurity culture** mean for an entrepreneur? How to implement it?

- ☑ Develop a cybersecurity policy covering people, processes and technology, with the focus on people
- ☑ Dedicate time during all-hands-on meetings to assess the state of the organization's cybersecurity issues and updates
- ☑ Provide continuous employee training on cybersecurity matters and regularly test their knowledge and awareness
- ☑ Build products with security in mind and focused on customer and user needs
- ☑ Communicate the importance of cybersecurity and privacy to the whole organization
- ☑ Ensure that there is cybersecurity expertise among employees and organizational leadership
- ☑ Demonstrate commitment to security best practices such as identity and access management, multifactor authentication, data protection, layered endpoint and network defence
- ☑ Include a cybersecurity strategy in the business plan and strategy
- ☑ Establish a communication channel for security-related topics

What does **cybersecurity culture** mean for an investor? How to validate it?

- ☑ Request evidence-based data of employee training and their understanding of cybersecurity matters
- ☑ Request the results of latest penetration tests performed on a target company's network
- ☑ Request examples of how security is integrated in the early stages of product or system planning and the development process
- ☑ Emphasize the importance of a target's cyber preparedness and culture as part of a successful growth path
- ☑ Validate that target company leadership understands cyber risks and has a plan to manage and mitigate them

4.2 Cybersecurity governance

Long-term success in the Fourth Industrial Revolution is not possible without a comprehensive cybersecurity strategy.[27] Cybersecurity governance is an essential component of business strategy for building a sustainable and successful business. Organizational cybersecurity cannot be left to the cybersecurity team alone, every employee must engage. Ultimately, the board takes responsibility for oversight of cyber risk and resilience.

While it is everyone's responsibility to play their part in ensuring robust cybersecurity, the ultimate responsibility lies with executives who set the strategy of an organization. Successful cybersecurity governance starts with the highest-level leadership recognizing the importance of their role in prioritizing security and privacy in the business strategy. In recent years, such leaders have increasingly been held liable for incorporating cybersecurity into their business strategy. Boards and senior management play a critical role in determining how cybersecurity is integrated across all business operations through informed decision-making and targeted investment.

Cybersecurity governance is a subset of a corporate governance that provides a strategic direction for cybersecurity activities and oversight of cybersecurity risk. When done well, cybersecurity governance effectively coordinates the security activities of the company and enables the flow of security information and decisions.

Good cybersecurity governance should:

1. Clearly link security activities to the organization's goals, priorities and business strategy
2. Identify the individuals responsible at each level for making security decisions and empower them
3. Ensure accountability for decisions
4. Ensure that feedback is provided to decision-makers on the impact of their choices
5. Fit into an organization's wider approach to governance and risk
6. Develop and approve a security budget
7. Align incentives for cybersecurity training

Good cybersecurity governance also means scheduling regular cyber-risk reviews and cybersecurity updates as business develops so that cybersecurity experts can update C-Suite and corporate management. These meetings should focus on cyber-risk assessments, tabletop exercises running through different incident response plans, discussion of any related budgetary needs and proposed training sessions for the company.

> *We see two types of early stage companies: the ones that treat cybersecurity as a checkbox compliance issue, and the ones that understand that it is fundamental to maintain the trust of clients. If an emerging company fully commits to cybersecurity, then its commitment will be rewarded by market confidence and consumer trust. The cyber essentials provide a pathway to any entrepreneur and business leader to implement cybersecurity in the fabric of major enterprises and deliver innovation in a secure way.*

Craig Froelich
Chief Information Security Officer
Bank of America
USA

What does **cybersecurity governance** mean for an entrepreneur? How to implement it?

- ☑ Develop a cybersecurity strategy, programme and risk model
- ☑ Consider cybersecurity as a business enabler, driving growth by gaining and ensuring the trust and confidence of customers and consumers
- ☑ Organize quarterly meetings between the cybersecurity expert/s and key stakeholders, including C-Suite and corporate management
- ☑ Hold regular threat intelligence briefings to inform the leadership on the cyberthreats their industry is confronting
- ☑ Create a cybersecurity review board with key personnel from across the organization to help broaden awareness and ensure a smooth decision-making process
- ☑ Ensure your organization connects with various cybersecurity industry associations and leverages their network of peers
- ☑ Include cyber-risk issues as a regular discussion item on the board meeting agenda
- ☑ Promote the importance of security and privacy to your organization to foster a culture of security and privacy among employees
- ☑ Conduct routine penetration tests and code reviews to catch security flaws in the development cycle
- ☑ Create highly visible ways for employees to report any security-related matters and issues

What does **cybersecurity governance** mean for an investor? How to validate it?

- ☑ In the early stage of investment negotiations, the investor should clearly define ongoing cybersecurity expectations, benchmarks and incentives within investment mandates and term sheets
- ☑ Identify what cybersecurity policy framework the target company uses
- ☑ Understand the corporate structure and who is responsible for cybersecurity strategy and implementation
- ☑ Include cybersecurity issues on the board meeting agenda
- ☑ Investigate whether the corporate leadership emphasizes cybersecurity in their risk-related discussions
- ☑ Request for the open source code scans and code reviews to review potential security vulnerabilities
- ☑ Ensure the right cybersecurity expertise is represented on the board
- ☑ Use independent third-party service to understand the external security landscape of the target company, then based on this data hold interviews with the key stakeholders of the target company
- ☑ Ask for cybersecurity training reports, including phishing email campaign results and online training participation
- ☑ Ensure the target company can clearly articulate their top cyber risks and what it is doing to reduce, manage and mitigate them
- ☑ Map out the entire legal and regulatory compliance landscape of the target company and ensure that they have concrete compliance accordingly
- ☑ Understand the target company's assets and the risks associated with them
- ☑ Enquire about the expected financial costs of a data breach and compare them to the insurance coverage

4.3 Cyber resilience

With most organizations today relying on digital technology to function, cyber resilience must be integrated into operational resilience and business continuity risk management. Cyber resilience refers to the organization's ability to prepare, respond to and recover from a cyberattack, a network breakdown or a data breach incident when they occur. The purpose of robust cyber resilience is to maintain the confidentiality, integrity and availability of data and to ensure business operation continuity.

If cybersecurity is primarily about protecting an organization, cyber resilience is about quickly recovering and thriving when that protection fails, as it inevitably will at some point in time. While prevention is important, cybersecurity experts know that there is no bulletproof method to thwart potential attacks, especially as bad actors increasingly apply new emerging technologies that circumvent cyber defences.[28] For this reason, a company's ability to continuously deliver the expected services and operations despite adverse cyber events or system failures is becoming an important factor in corporate cyber preparedness.

A well-prepared, updated and regularly tested incident response plan is essential to cyber resilience. For optimal accuracy, cybersecurity teams must practice drill their incident response plan regularly, actively involving executives across the technology, legal, human resources, investor relations, compliance and risk management departments. Regular drills ensure that every executive knows their role and responsibilities in the incident response process. Moreover, an incident response plan determines the scope of a breach, clarifies how to notify clients and investors, lists how to meet legal and compliance requirements, and provides guidelines for internal and external communications. Even the most mature and sophisticated plans are effective only if they have been sufficiently tested.[29] Neglecting to do so leaves potential shortcomings or blind spots unaddressed, creating vulnerabilities for bad actors to exploit in potential attacks.[30]

The following recommendations make for strong cyber resilience:

1. Penetration tests to simulate attacks on a computer system, network or application to identify security vulnerabilities that could be exploited
2. Phishing tests, social engineering training and assessments to engage staff in recognizing cyber threats
3. Vulnerability tests to review any potential weaknesses within the internal network and product, particularly focusing on how well a system works under attack
4. Incident response exercises for key personnel to practice their responsibilities in the event of a successful cyberattack
5. A compromise assessment, to ascertain the indicators of a successful compromise
6. A robust back-up system should any downtime occur, to always be ready to quickly and seamlessly switch to a back-up service

Each of these assess and ensure various components of a company's cyber preparedness to provide essential assurances that the system's programmes and protocols are effective and have not been compromised. Ultimately, the goal of the compromise assessment is to identify any adversarial activity or malicious logic. Organizations must build robust cyber capabilities to protect, detect and respond to a cyber incident or a system failure. The response is the most important factor of well-managed cyber resilience.

What does **cyber resilience** mean for an entrepreneur? How to implement it?

- ☑ Develop an incident response plan, test and run regular incident-response training
- ☑ Ensure that corporate management is included in tabletop exercises
- ☑ Develop an ability to monitor and observe the networks with an emphasis on incident response. Understand your organization's mean time to detect, mean time to contain and mean time to remediate the key elements of resilience
- ☑ Conduct ongoing security awareness activities for all employees at least several times a year
- ☑ Back up corporate data regularly. Automatic daily backups are ideal
- ☑ Store regularly updated data backups on a separate network so that the compromised data can be restored quickly
- ☑ Create a cybersecurity taskforce and communicate contact details of everyone on the taskforce in the organization, so that staff know who to contact when a cybersecurity incident occurs
- ☑ Secure robust cyber insurance coverage and leverage an insurer's vendors in the event you rapidly need to deploy cyber forensics, incident response, legal advice, regulatory engagement and crisis communication experts

What does **cyber resilience** mean for an investor? How to validate it?

- ☑ Check whether the target has a cybersecurity incident response plan and whether it has been practiced
- ☑ Check whether cybersecurity incident response exercises have been done and request a report on them
- ☑ Investigate whether a target company has suffered a cybersecurity incident, how it responded, and what were the lessons learned
- ☑ Request an assessment report, proof of vulnerability management and patching reports
- ☑ Consider purchasing a cyber insurance policy as part of managing the target company's cyber risk
- ☑ Compare the target's cyber insurance policy to the expected cost of a cybersecurity incident

4.4 Security-by-design

To create a safer cyberspace, security must be prioritized throughout the product development cycle. The security-by-design approach to software and hardware development seeks to minimize system vulnerabilities and reduce the attack surface by designing and incorporating security into every part of the development process. As per OWASP[31], products and systems developed without security are like bridges constructed without finite element analysis and wind tunnel testing. They look like bridges, but they will fall at the first flutter of a butterfly wing.

Security-by-design must be incorporated from the outset of the product development cycle to prevent any security retrofitting or discovery of major security vulnerabilities at later stages of product development. To add security features and revise a product and its algorithm becomes far costlier at later stages. By incorporating security features as a design criterion, entrepreneurs and innovators minimize the number of vulnerabilities and diminish the attack surface in the development process. Too many innovators still treat security as an afterthought in the development process. Addressing in-built vulnerabilities and patching built code can be a cumbersome process and is quite costly. More importantly, it is never as effective as designing systems to be secure from the get-go. To prioritize security features from the beginning of product development is a cost-conscious and more expedient approach than adding them on later in the product life cycle.

Security-by-design is a much broader commitment to building secure products than solely identifying and fixing vulnerabilities, important though they are. Security teams need to be empowered if they are to successfully implement the security-by-design principle in new software and systems, to secure their architectures by design. This implies a higher level of coordination and oversight with the product development team, calling for the security development team to be included in the overall product and system development process from the start. Secure design also implies that designers of the software and systems are trained in applied security principles, to equip them with the tools and knowledge they need to effectively implement security features, reduce and harden the attack surface, and layer multiple security mechanisms into the design.

Far more than best practice, security-by-design has become a legal requirement for all organizations that operate in the European Union or are accessing the data of European citizens and will need to be operationally demonstrable. Both the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR) of the European Union require integration of security throughout the entire development life cycle – starting from the design of requirements to maintenance.

Moreover, the GDPR has extraterritorial applicability outside the European Union when targeting or monitoring EU citizens.

> *"Technology companies play a vital role in protecting our networks, enterprises and national infrastructure with a mix of innovation and education. Enterprises must understand that cybersecurity is a shared responsibility and the proposed cyber essentials provide clear and practical guidance to help companies of all types prioritize and implement security best practices. Similarly, entrepreneurs and innovators developing new products should prioritize privacy- and security-by-design principles to ensure the longevity and durability of their technology."*
>
> **Joram Borenstein**
> General Manager, Cybersecurity Solutions Group
> Microsoft
> USA

What does **security-by-design** mean for an entrepreneur? How to implement it?

- ☑ Incorporate security-by-design into the quality assurance (QA) process of a product life cycle
- ☑ Urge the development operations team to include security in their development process from the start
- ☑ Consider all the ways that potential threats could impact the product or service and have a plan for those potential interruptions
- ☑ Scan all open-source and third-party code components for known vulnerabilities and misconfigurations
- ☑ Map out where the data is coming from and investigate whether and how the data could be manipulated
- ☑ Incorporate the principle of defence in depth (DiD) through secure coding practices
- ☑ Perform threat modelling to understand any potential threats to the product or system
- ☑ Build a security test plan that involves specialized personnel and tools that are beyond the normal function of a quality assurance (QA) team
- ☑ Ensure that code reviews for security purposes are performed as part of product development
- ☑ Incorporate mandatory and seamless security and compliance testing as part of the product development process

What does **security-by-design** mean for an investor? How to validate it?

- ☑ Verify that security-by-design is adequately considered in the product's development process. Interview the product development managers and designers
- ☑ Ascertain whether the target company has considered key risks at an early stage of the product roadmap
- ☑ Request penetration test results for the product(s) or system(s) that the target company is developing
- ☑ Request the provenance of code (aka Software Bill of Materials) to audit a software's chain of custody and origins

4.5 Privacy-by-design

In recent years, consumers have lost trust in the ability and intention of companies to ensure data privacy. Millions of personal identifiable information data sets have been leaked, hacked and lost in a growing number of colossal global breaches. As a recent global survey on internet security shows[32], the trust deficit is widening around the globe and causing people to change the way they behave online. Survey results report that 78% of respondents were concerned about their online privacy, 49% disclosed less personal information online owing to distrust online and 43% are taking meaures to secure their devices. Without user trust, companies will be challenged to continue accessing vast amounts of data for building better products or teaching machines.

Organizations that handle their customer data with care will be rewarded and those that do not risk the loss of reputation, damage to their brand and dissatisfying their customers. In other words, they risk loss of business. Privacy-by-design means establishing respect for privacy as a foundational tenant of the product development life cycle. Privacy must be a priority consideration in every step of the process – from the initial whiteboard stage through design, development, quality assurance and product release. As with security, from best practice privacy-by-design has become a legal requirement for organizations that operate in the European Union or are accessing the data of European citizens, and it must be operationally demonstrable.

The GDPR requires organizations to incorporate privacy at the earliest stage of the development process. Privacy must be an integral component of a new product or service, not an add-on. This might seem complex, but it is in fact easier than applying privacy considerations after a product or a system is fully developed. Considering upfront what personal data will be used, for what purpose and how it will be collected in a legitimate way reduces the likelihood of discovery at a later stage that embedding privacy is technologically challenging, expensive or even impossible. Entrepreneurs and innovators will succeed and ensure consumer trust by incorporating data protection as an essential component of their product offering. This involves ensuring that personal data is automatically protected in any information technology system, service, product and business practice, so that users are not required to take any specific action to protect their privacy.[33] Building a product or service with strong privacy default settings and user-friendly controls will enhance user trust and loyalty.

The privacy-by-design principle includes simple steps like communicating with users in accessible and plain language providing clear guidance on the purpose of collecting their personal data. Privacy-by-design is a cornerstone principle of the human-centric approach to innovation. Its purpose is to keep and respect user needs and privacy at the core of the entire product development process.

What does **privacy-by-design** mean for an entrepreneur? How to implement it?

- ☑ Remind users on a regular basis that their data is collected and shared, and inform them of how it is used; allow users to opt out
- ☑ Apply anonymization of data as a possible protective measure
- ☑ Include data protection requirements in the design and development of business systems, services and products
- ☑ Assign a qualified employee to be responsible for the data protection policy and its implementation
- ☑ Prioritize minimization of sensitive data collection
- ☑ State clearly and directly what data is collected and how it will be used
- ☑ Ensure implementation of measures to meet customer requests for “the right to be forgotten”
- ☑ Carry out a privacy-impact assessment before launching any new product or a product update
- ☑ Incorporate privacy-by-design in the product development QA process

What does **privacy-by-design** mean for an investor? How to validate it?

- ☑ Ascertain the value of collected data at the target company. How much does it cost to collect data and compare this cost to the actual usefulness of the data versus the liability in case of a data leak or breach
- ☑ Request proof of data collection and check that anonymization and minimization measures are applied to data collection
- ☑ Verify the privacy policy of the target company
- ☑ Confirm that privacy is incorporated in the product development life cycle
- ☑ Verify whether expired or outdated data is deleted by the target company

4.6 Data governance and protection

Well-organized data governance is a requirement of business compliance, voluntarily or as stipulated by industry standards, government regulations or international treaties. Data governance plays an essential role in managing and maintaining the availability, usability, integrity and security of enterprise data.

Data protection, especially data that is personal identifiable information, is one of the most regulated elements of cybersecurity. It is an important component of an increasingly data-driven economy as it reduces exposure to unnecessary risks and allows for the building of trusted relationships with customers and commercial partners. It ensures consumer trust in product and service providers, drives innovation and enables digital transformation. Failure to conduct effective data protection measures can result in consumer identity theft, leaks of sensitive data, discrimination of individuals, and in-built bias. Data protection has become a truly global concern and action as people around the world increasingly cherish and value the protection and security of their data. Regulations such as the GDPR and the California Consumer Privacy Act (CCPA) aim to hold organizations and their executives more accountable than ever before for the protection of information and data, and they define how to use customer data in a responsible manner.

Data protection refers to the practices, safeguards and binding rules enacted to protect information and maintain its confidentiality, integrity and availability. Data and information protection make a point of maintaining the confidentiality, integrity and availability of all-important information for an organization, its employees, customers and third parties. According to a recent Accenture study, a new wave of cyberattacks sees data not only being stolen, but also manipulated or destroyed, which inevitably breeds distrust.[34] Moreover, the study claims that attacking data integrity is the next focus area for cyber criminals.

Every organization should develop and maintain a data protection policy – a set of principles, rules and guidelines that outline how an organization will ensure ongoing compliance with data protection laws. Data protection is no longer an issue that sits with the legal department. It has become an overarching principle for which every employee in an organization is responsible and accountable. Executives, engineers, product designers, product developers and lawyers have to possess the same level of understanding of what data the company is gathering and why, what data protection entails, like maintaining data inventory, knowledge on how and when to eliminate data when it is not needed. With the right technology, data governance and protection drive enormous business value and support digital transformation. For all these reasons, it is therefore important to involve all staff in ensuring an efficient data governance strategy and model.

What does **data and information protection** mean for an entrepreneur? How to implement it?

- ☑ Develop and maintain a data protection policy, including a written and comprehensive information security programme to ensure the security, confidentiality and integrity of personal data held
- ☑ Appoint a data protection officer who would issue an annual report to the board
- ☑ Consider establishing a data protection working group drawing stakeholders from across the business, product development and engineering teams to take responsibility for the day-to-day management of data protection and compliance
- ☑ Use encryption for data storage at rest and data in transfer
- ☑ Ensure that staff understand the importance of data protection and are committed to it
- ☑ Limit sensitive data storage to selected drives only and provide access to those drives only to selected and vetted employees

What does **data and information protection** mean for an investor? How to validate it?

- ☑ Verify whether a target company has a data protection policy and whether it complies with the required regulations, according to their industry, geographical outreach, collected data and the nature of their business
- ☑ Understand all required regulations and policies with which the target needs to comply
- ☑ Verify whether a target company has a data protection officer or a committee responsible for data protection
- ☑ Ensure that the target company has mapped out all its data and information flows, whether on premises or on cloud
- ☑ Question target company management about which data regulations the company is subject to and what steps they have taken to ensure compliance

4.7 Third-party security

Third-party security focuses on protecting an organization against cybersecurity threats that originate from the supply chain, vendors or customers. Considering the explosive growth of outsourced technology services in corporate technology infrastructure and development of innovation, companies must control and master their third-party exposure by implementing safeguards and processes to mitigate their vulnerability. A corporate network is only as secure as the networks of its vendors and supply chain. The third-party ecosystem is an ideal environment for cyber criminals to access any organization almost unnoticed. To outwit cybercriminal activity, executives need to cooperate on plans for third-party risk detection and mitigation that are built on strong governance practices. Third-party cyber-risk management entails understanding the risks posed by corporate relationships with vendors, and strategically deploying data and automation to make the most of human capital.

A significant 44% of companies had experienced a business-altering data breach caused by a vendor.[35] Data shows that companies are lagging far behind on instituting the governance and technology to manage their third-party risks, whether in the software supply chain, access governance or data handling.

An average company often works with tens, if not hundreds of vendors, including service providers and subcontractors with whom it shares data to improve service delivery and reduce costs. The vendors have varying degrees of cyber preparedness and present variable degrees of risk depending on the data to which they have access and store. In many circumstances, the third parties are effectively custodians of the original information, and it is critical to clarify their methods of safeguarding the data further down the value chain. Considering the pronounced risks in terms of the practices or cyber unpreparedness that third parties may present, organizations must accurately assess vendors based on their risk profile and cyber readiness and, in turn, apply the appropriate level of rigour to their transactions with each.

Third-party security analysis tasks aim to identify any potential and existing threats, protect against standard attack vectors, detect any potential data breaches, and plan for asset recovery. Some of critical tasks include:

1. Performing a vigorous annual vendor assessment
2. Mapping data flows, in both physical and digital forms
3. Assessing how third parties safeguard data
4. Using leading practices and industry standards
5. Monitoring ongoing vendor interactions
6. Defining each vendor's criticality and understanding what data or network parts they have access to

One important security matter to address when mapping out third parties is the application programming interface (API) network. Businesses that collect, store and share data through APIs should prioritize security when they open it up to third parties to ensure that their digital supply chain is visible and secure. APIs are the nexus of significant emerging technology areas, such as software as a service (SaaS), big data, machine learning and artificial intelligence.[36] Through APIs, third parties gain access to user-related data that can be used to create new value. If not administered well, however, these interchanges become a vulnerability and result in data leakage.[37] To ensure that security is monitored when deploying the APIs, businesses need to develop an API deployment guide and framework. It should incorporate security-by-design principles, prioritize access protection and control, and leverage proven security standards stores for authentication and authorization.[38]

What does **third-party security** mean for an entrepreneur? How to implement it?

- ☑ Develop a third-party cyber-risk management framework
- ☑ Designate third parties as low-, medium- and high-risk, according to their access to potentially sensitive areas of operations and data
- ☑ Use technological solutions to gain an independent, continuous assessment of third-party security posture
- ☑ Apply the “trust but verify” principle when dealing with third parties
- ☑ If a company is using, incorporating or buying any external code as part of their technology development, the code must be actively validated, tracked and updated as needed
- ☑ Extend your corporate cybersecurity practices to third parties like suppliers, partners and customers
- ☑ Develop API deployment guidelines and ensure that third parties with access to confidential information have appropriate and active security standards and measures
- ☑ Require key vendors to have a cyber insurance policy

What does **third-party security** mean for an investor? How to validate it?

- ☑ Ensure that the target company has an established third-party risk programme, including a clear understanding of its data flows
- ☑ Request a map of the target company’s digital and physical supply chain, to determine to which digital channels third parties have access
- ☑ Validate any due diligence documents to detect the types and amount of risk the third parties pose to the target company

5. Conclusion

With the economy and society growing ever more dependent on technology and particularly so in the COVID-19 pandemic, the security and privacy of our digital tools are more important than ever, as is ensuring the confidentiality, integrity and availability of data. With the dissemination of the cyber essentials in this report, the World Economic Forum seeks to provide guidance to entrepreneurs and investors determined to develop responsible, sustainable and secure technology and practices.

The cyber essentials focus on improving the security baseline across technology innovation. Over time, implementing the fundamentals of prioritizing security and privacy features in technology will reduce the frequency, scale and success of cyberattacks and breaches, ultimately resulting in substantially more robust cybersecurity across industries and geographies. Entrepreneurs and investors have a responsibility, proportionally to the rate of dependency on technology, to commit to and develop secure and inclusive technology that benefits users.

Incorporating cybersecurity in technology from the very start of its development is no longer an option; it underpins the survival and stability of our economic systems, the transparency, sustainability and trust in our communication tools, it is a matter of national security. History is full of examples where security was not given due consideration in innovation until inventions like cars, airplanes and drugs became so widely used that their security features could not be ignored. From an afterthought, after years of development and progress security has become a success-defining element of innovation. Who does not consider the safety features and rating when buying a car? Who would choose to fly if there were not an almost 100% success rate in safe take-off and landing? Medicines would not pass clinical trials to reach the market without meeting safety standards.

The technology is here to stay and flourish. We cannot envision, nor are there any “digital rollback” plans. Consequently, entrepreneurs and innovators have a responsibility to respect technology as an essential component of our daily lives and consumers must demand requisite security and safety standards as they do of other essential products and services.

The pressing cybersecurity challenges of our age cannot be solved by any one group – collaboration is crucial. The technology innovation path starts with an inventor, an entrepreneur and is supported by investors to ensure its success. All stakeholders involved in introducing new products, applications, platforms and technology services are responsible for ensuring that next-generation technology provides more security and privacy features for consumers than did the previous iteration.

The evolution of cybersecurity has been and will continue to be a fascinating combination of technology features, data reliability, laws and incentives. To ensure it is a priority in any technology development, public-private collaboration is essential. The World Economic Forum provides these cyber essentials for public and private sector leaders to urge prioritization of cybersecurity and robust cyber resilience.

An overwhelming majority of executives continue to be largely dissatisfied with the effectiveness of their cybersecurity spending, often all too myopically focused on the newest technologies. A strategic trade-off needs careful consideration to benefit fully from the combined power of cyber innovation, while minimizing the threat and enabling the people to perform effectively.

Benjamin Haddad
Director
Accenture Ventures
Israel

We developed a baseline for cyber preparedness and practical recommendations for entrepreneurs and innovators to help prioritize and implement cybersecurity by applying cyber essentials to their strategy. By applying these cyber essentials, business leaders incorporate cybersecurity into the business strategy and develop a unified cybersecurity approach across all business units.

Derek Vadala
Chief Executive Officer
Cyber Assessments
USA

Investors are increasingly evaluating the cyber risk of target investments as part of the overall due diligence process. Security is a smart investment, especially where companies are innovating and developing new technologies. It ensures their product durability and resilience, and customers expect security-by-design.

Adam Fletscher
Chief Information Security Officer
Blackstone
USA

Contributors

Lead Authors

Algirde Pipikaite	Project Lead, Industry Solutions, Platform for Shaping the Future of Cybersecurity and Digital Trust, World Economic Forum

Contributors

Benjamin Haddad	Director, Accenture Ventures, Israel
Anup Ghosh	Managing Director, Accenture, USA
Carrie Gates	Senior Vice President, Global Information Security, Bank of America, USA
Craig Froelich	Chief Information Security Officer, Bank of America, USA
David Ritenour	Chief Information Security Officer, BlackRock, USA
Adam Fletcher	Chief Information Security Officer, Blackstone, USA
Sawan Ruparel	Engineering Lead and Venture CTO, BCG Digital Ventures, USA
Jason Min	Head of Business and Corporate Development, Check Point Software Technologies, USA
Chris Merritt	Chief Revenue Officer, Cloudflare, USA
Michelle Zatlyn	Co-Founder and Chief Operating Officer, Cloudflare, USA
Einaras von Gravrock	Chief Executive Officer, CUJO AI, USA
Derek Vadala	Chief Executive Officer, Cyber Assessments, USA
Pascal Millaire	Chief Executive Officer, CyberCube, USA
Sahil Segal	Startup & Innovation Lead, Deloitte, USA
Jason Harrell	Head of Business and Government Cybersecurity Partnerships, Depository Trust & Clearing Corporation, USA
Wilson Henriquez	Head of International Business Security, Equifax, USA
Bhakti Mirchandani	Managing Director, FCLT Global, USA
Edlyn Victoria Levine	Research Associate, Department of Physics, Harvard University, USA
Syam Thommandru	Global Head of Product Management, Strategic Alliances and Cybersecurity, HCL Technologies, United Kingdom
Kenneth Goldman	President, Hillspire, USA
Kelly Young	Chief Information Officer, Hillspire, USA
Christine Riccardi	Regional Director, Cybersecurity and Infrastructure Security Agency, USA
Katheryn Rosen	Global Head, Technology and Cybersecurity Policy and Partnerships, JPMorgan Chase & Co., USA

Matthew Goldstein	Partner, M12, Microsoft's Venture Fund, USA
Joram Borenstein	General Manager, Cybersecurity Services, Microsoft Corporation, USA
Marc Barrachin	Managing Director, Product Research and Innovation, S&P Global Market Intelligence, USA
Martina Cheung	President, S&P Global Market Intelligence, USA
Jim Alkove	Chief Trust Officer, Salesforce, USA
David Li	Executive Director, Shenzhen Open Innovation Lab (SZOIL), People's Republic of China
Haiyan Song	Senior Vice President, Security Markets, Splunk, USA
Lluis Pedragosa	General Partner and Chief Financial Officer, Team8, USA
Burke Norton	Senior Managing Director, Vista Equity Partners, USA

From the World Economic Forum

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

Endnotes

1. World Economic Forum. 2020. *The Global Risks Report 2020, 15th Edition.* p. 62. https://www.weforum.org/reports/the-global-risks-report-2020 (link as of 5/5/2020)

2. World Economic Forum. 2020. COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications. p. 8. https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications (link as of 02/06/2020

3. World Economic Forum. 2020. *The Global Risks Report 2020, 15th Edition.* p. 62. https://www.weforum.org/reports/the-global-risks-report-2020 (link as of 27/03/2020)

4. Redman, Thomas and Waitman, Robert. 2020. *Do You Care About Privacy as Much as Your Customers Do?* Harvard Business Review. https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do (link as of 06/05/2020)

5. Schwab, Klaus. 2016. *The Fourth Industrial Revolution: what it means, how to respond.* World Economic Forum. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ (link as of 27/03/2020)

6. S&P Global. 2020. *Businesses Bracing for Major Disruptions from COVID-19 according to S&P Global Market Intelligence Survey.* http://press.spglobal.com/2020-03-26-Businesses-Bracing-for-Major-Disruptions-from-COVID-19-according-to-S-P-Global-Market-Intelligence-Survey (link as of 27/03/2020)

7. Accenture Security. 2019. *The Cost of Cybercrime. 9th Annual Study.* p. 8. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (link as of 27/03/2020)

8. Accenture Security. 2019. *The Cost of Cybercrime. 9th Annual Study*. Accenture Security. p. 8. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (link as of 27/03/2020)

9. World Economic Forum. 2020. *The Global Risks Report 2020, 15th Edition*. p. 62. https://www.weforum.org/reports/the-global-risks-report-2020 (link as of 27/03/2020)

10. Hung, Mark. 2017. *Leading the IoT: Gartner Insights on How to Lead in a Connected World.* Gartner. p. 2. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf (link as of 27/03/2020)

11. International Data Corporation (IDC). 2019. *The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast*. https://www.idc.com/getdoc.jsp?containerId=prUS45213219 (link as of 20/05/2020)

12. Technology.org. 2019. *Cyberattacks on IoT Devices Grow 300% in 2019: How to Secure Yourself?* https://www.technology.org/2019/11/19/cyberattacks-on-iot-devices-grow-300-in-2019-how-to-secure-yourself/ (link as of 27/03/2020)

13. IBM Security. 2019. *Cost of Data Breach Report.* https://databreachcalculator.mybluemix.net (link as of 27/03/2020)

14. The World Bank. 2020. *Small and Medium Enterprises (SMEs) Finance.* www.worldbank.org/en/topic/smefinance (link as of 27/03/2020)

15. Pipikaite, Algirde and Song, Haiyan. 2019. *What Do Hurricanes and Cybersecurity Have in Common?* Scientific American. https://blogs.scientificamerican.com/observations/what-do-hurricanes-and-cybersecurity-have-in-common/ (link as of 27/03/2020)

16. Cleaveland, Ann, Weber, Steve and Phelps, Bill. 2020. *Resilient Governance for Boards of Directors. Considerations for Effective Oversight of Cyber Risk.* Center for Long-Term Cybersecurity. p. 20. https://cltc.berkeley.edu/wp-content/uploads/2020/01/Resilient-Governance-for-Boards-of-Directors-Report.pdf (link as of 27/03/2020)

17. The Brazilian General Data Protection Law (LGPD) or "Lei Geral de Proteção de Dados" in Portuguese, was approved in August of 2018 and went into effect in February 2020.

18. Red Alert Labs. 2018. *The Importance of Security by Design for IoT Devices.* https://www.redalertlabs.com/blog/the-importance-of-security-by-design-for-iot-devices (link as of 05/05/2020)

19. World Economic Forum. 2019. *Incentivizing Responsible and Secure Innovation: Principles and guidance for investors.* p. 5. https://www.weforum.org/reports/incentivizing-responsible-and-secure-innovation-principles-and-guidance-for-investors (link as of 27/03/2020)

20. Forescout. 2019. Forescout Study Reveals Cybersecurity Concerns on the Rise Amid M&A Activity. Forescout Technologies, Inc. https://www.forescout.com/company/news/press-releases/forescout-study-reveals-cybersecurity-concerns-on-merger-and-acquisition-activity/ (link as of 27/03/2020)

21. World Economic Forum. 2019. *Incentivizing Responsible and Secure Innovation: Principles and guidance for investors.* https://www.weforum.org/reports/incentivizing-responsible-and-secure-innovation-principles-and-guidance-for-investors (link as of 27/03/2020)

22. World Economic Forum. 2019. *Incentivizing Responsible and Secure Innovation: Principles and guidance for investors.* https://www.weforum.org/reports/incentivizing-responsible-and-secure-innovation-principles-and-guidance-for-investors (link as of 27/03/2020)

23. Küderli, Urs. 2018. *The journey to digital trust.* PWC. https://www.pwc.ch/en/insights/digital/digitaltrustinsights.html (link as of 27/03/2020)

24. Spadafora, Anthony. 2019. *90% of data breaches are caused by human error.* Techradar Pro. https://www.techradar.com/news/90-%-of-data-breaches-are-caused-by-human-error (link as of 7/5/2020)

25. ISACA. 2018. *The 2018 Cybersecurity Culture Report.* ISACA and CMMI Institute. https://www.isaca.org/-/media/info/cybersecurity-culture-report/index.html (link as of 27/03/2020)

26. ISACA. 2018. *The 2018 Cybersecurity Culture Report.* ISACA and CMMI Institute. https://www.isaca.org/-/media/info/cybersecurity-culture-report/index.html (link as of 27/03/2020)

27. Schwab, Klaus. 2016. *The Fourth Industrial Revolution: what it means, how to respond.* World Economic Forum. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ (link as of 27/03/2020)

28. McDonough, Bart. 2019. *Commentary: Why cybersecurity governance is essential for institutional investors.* Pensions & Investments. https://www.pionline.com/article/20190321/ONLINE/190329985/commentary-why-cybersecurity-governance-is-essential-for-institutional-investors (link as of 05/05/2020)

29. McDonough, Bart. 2019. *Commentary: Why cybersecurity governance is essential for institutional investors.* Pensions & Investments. https://www.pionline.com/article/20190321/ONLINE/190329985/commentary-why-cybersecurity-governance-is-essential-for-institutional-investors (link as of 05/05/2020)

30. McDonough, Bart. 2019. *Commentary: Why cybersecurity governance is essential for institutional investors.* Pensions & Investments. https://www.pionline.com/article/20190321/ONLINE/190329985/commentary-why-cybersecurity-governance-is-essential-for-institutional-investors (link as of 05/05/2020)

31. OWASP Foundation. 2016. *Security by Design Principles.* OWASP Foundation Wiki. https://www.owasp.org/index.php/Security_by_Design_Principles (link as of 27/03/2020)

32. *2019 CIGI-Ipsos Global Survey on Internet Security and Trust.* The survey was conducted in 25 economies: Australia, Brazil, Canada, China, Egypt, France, Germany, Hong Kong SAR, India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, Russian Federation, South Africa, Republic of Korea, Sweden, Tunisia, Turkey, the United Kingdom, and the United States.

33. Information Commissioner's Office, the United Kingdom. 2018. *Data protection by design and default.* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (link as of 13/05/2020)

34. Accenture Security. 2019. *The Cost of Cybercrime. 9th Annual Study.* p. 6, https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (link as of 27/03/2020)

35. Sangster, Mark. 2019. *Nearly half of firms suffer data breaches at hands of vendors.* Help Net Security. https://www.helpnetsecurity.com/2019/04/24/nearly-half-of-firms-suffer-data-breaches-at-hands-of-vendors/ (link as of 07/05/2020)

36. Pipikaite, Algirde. 2018. *How to stop data leaks.* World Economic Forum. https://www.weforum.org/agenda/2018/11/how-to-stop-our-leaky-data-connections/ (link as of 05/05/2020)

37. Pipikaite, Algirde. 2018. *How to stop data leaks.* World Economic Forum. https://www.weforum.org/agenda/2018/11/how-to-stop-our-leaky-data-connections/ (link as of 05/05/2020)

38. Pipikaite, Algirde. 2018. *How to stop data leaks.* World Economic Forum. https://www.weforum.org/agenda/2018/11/how-to-stop-our-leaky-data-connections/ (link as of 05/05/2020)

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