WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Centre for Cybersecurity

Incentivizing responsible and secure innovation

Principles and guidance for investors

July 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

REF 65857

Contents

Preface

Alois Zwinggi
Member of the Managing Board
Head of the Centre for Cybersecurity
World Economic Forum

The governance of cyber risk is a key challenge for leaders in all sectors and industries. Companies, governments, academics and civil society must focus on developing mechanisms to meet or mitigate these new risks, individually and in global collaboration, to defend our shared networks, institutions and innovation itself.

The World Economic Forum's work on improving global cybersecurity governance is led by the Centre for Cybersecurity. Governance, in this context, refers to high-level solutions and recommendations that impact law, norms, markets and technology architecture[1] in order to support and foster security, resilience, integrity and trust.

Markets, including insurance and investment, are an important governance mechanism as society grows increasingly dependent on digital technologies. Software and technology companies have a vital role in securing the global cyber domain. Digital networks are globally interconnected, and 85%[2] of these are run and maintained by the private sector. Consequently, the strategies and actions of these private actors have significant consequences for all of society.

The body of work on Incentivizing Secure and Responsible Innovation aims to shape market incentives that ensure more robust security and to help investors recognize their important role in safeguarding systemic cybersecurity and resilience. Succeeding in this effort requires being aware of the risks, roles and responsibilities as well as of tools based on principles for the investment and technology communities.

This insight report elaborates on recent work focused on enabling investors to prioritize security within their investment portfolio and target companies. The project team at the Centre for Cybersecurity has engaged with a diverse group of stakeholders to develop new ways of empowering oversight and a new assessment framework to ensure that technology companies prioritize security in their development and production.

Prioritizing cybersecurity will not happen overnight. Multiple market structures are required to ensure that technology companies prioritize cybersecurity by means of innovative methods to incentivize security or disincentivize insecurity. Ultimately, many new models of market incentives must be developed to ensure that the opportunities presented by the Fourth Industrial Revolution are fully embraced.

Foreword

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

All roads to a trusted digital future lead through security.

Building that future calls upon us to take cybersecurity seriously when we innovate and create new technologies. This report is the first in a series of collaborative efforts by the World Economic Forum, its partners and stakeholders to understand and share the incentives needed to ensure that, as we innovate, we do so in a responsible and secure way.

This is highly important, because companies currently do not have the right incentive structure to focus on security. The cybersecurity challenges that we face today have arisen because there has been no incentive to build better security in the past. With this body of work, we begin to change that.

This report focuses on security incentives for investors, but we cannot emphasize enough the need for the entire innovation ecosystem to work together on improving security and making security-by-design and security-by-default priorities for all. We start this work with guidance for investors because they have such an important role in deciding what technologies are created and which are implemented. But they are not the only responsible party. The public and private sectors must both find solutions to our many cybersecurity challenges and work together to implement them.

In the coming months, we look forward to the next steps in this workstream on incentivizing secure and responsible innovation. Along with our partners[3], we will publish additional resources to enable implementation of the high-level cyber principles for investors. More broadly, we will continue to bring together leaders from the investment community, technology companies, public investment agencies, regulators and representatives of civil society to work together on these vital issues.

Bringing together all these stakeholders is one key aspect of incentivizing secure innovation – there is a long way to go towards achieving our goals in securing our shared digital future. Together, however, we can succeed in ensuring that innovation is secure, responsible and, most importantly, trusted.

Investors need to learn that security is a smart investment and not an unnecessary cost. Digital innovation is transforming everyday devices into computers: cars, medical devices, household appliances, the power grid. What was once computer and information security is now everything security, and security failures now pose real risks to life and property. Incorporating cybersecurity assessment in investment processes and guiding entrepreneurs to prioritizing security results in safer – and less risky – products and services.

Bruce Schneier
Lecturer
Harvard Kennedy School of Government, USA

Investors need to be able to confidently assess cyber risk with the same rigour as other risks they analyse and manage – and that ability can be met only with a standard set of principles. The cybersecurity due diligence assessment framework is a great building block for this as it offers an industry standard that investors can use across the investment cycles to help their portfolio of companies improve their cyber exposure practices.

Martina Cheung
President
S&P Global Market Intelligence, USA

Cyber criminals work tirelessly to exploit weak points in technology infrastructures and behaviours of employees. Investors have a responsibility to ensure that innovators prioritize and embed cybersecurity features in product and platform development right from the beginning, and ensure an adequate level of cybersecurity training for their employees.

Walter W. Bohmayr
Senior Partner and Managing Director
Boston Consulting Group, Austria

Fiduciary duty for investors increasingly involves assessing cyber risk of target investments, monitoring and mitigating the cyber risk of portfolio companies. This involves developing internal cyber capabilities, building cybersecurity capacity across their portfolios, and acknowledging that cybersecurity is a business – rather than an IT – issue. Technological innovation developed with security in mind increases the likelihood of long-term success.

Bhakti Mirchandani
Managing Director
Focusing Capital on the Long Term (FCLTGlobal), USA

In the Fourth Industrial Revolution, when most businesses are relying on technology and data, understanding cyber risk when investing must be a part of the investor's risk appetite calculation process. Cybersecurity preparedness assessment acts as a reference when making investment decisions and the cybersecurity due diligence assessment framework is one of the tools to enable investors to evaluate cyber risk.

Kelly Young
Chief Information Officer
Hillspire LLC, USA

1. Introduction

While the Fourth Industrial Revolution[4] is enabling the transition to a digital world and unlocking previously untapped opportunities, it also presents a new set of challenges. The pace and scale at which we are introducing new technologies is increasing the cyber-attack surface for malicious actors to exploit. As a result, cyber-attacks have almost doubled in past five years[5] with no sign of slowing down. These cyber-attacks have spanned from infringement of privacy and confidentiality to, more recently, compromise of system integrity and accessibility. For example, the NotPetya ransomware incident was one of the largest cyber-attacks of all time, causing $10 billion[6] in damage to companies and affecting computers around the world. It infected multiple industries, from medical service providers to a major logistics company, A.P. Møller-Maersk, halting their operations for more than 10 days in 2017.[7] These cyber-attacks not only have a global economic impact, they also undermine overall trust in technology.

> Ooops, your important files are encrypted.
>
> If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
>
> We guarantee that you can recover all your files safely and easily. All you need to do is to submit the payment and purchase the decription key.

NotPetya's ransom note

To build and maintain trust in the digital domain, cybersecurity must be at the forefront of business strategy and innovation. It is vital that institutions continue innovating to extract the value that the Fourth Industrial Revolution brings. This innovation, however, must be conducted responsibly, with a focus on security.

Moreover, once a technological product has been released, it becomes difficult and more expensive to upgrade security, involving patching difficulties, complications arising from halt of operations for security upgrade, and so on. For these and other reasons, security needs to be integrated into the innovation strategy from the start, incorporated from design stage and engineered into every system and every component of every system, implemented from the very beginning and throughout the development process.[8]

In the long term, prioritizing security is in the interest of investors as they look to protect and increase their financial returns. The impact that cyber-attacks can have on business value is best showcased by Verizon Communication's recent acquisition of Yahoo. As a result of Yahoo disclosing two data breaches, Verizon reduced their acquisition price from $4.83 billion to $4.48 billion ($350 million price reduction).[9] Marriott International's acquisition of Starwood in 2016, followed by a detection of a cyber breach in Starwood's network, is another well-known example of investor loss due to cyber-attack. As a result of an identified security breach in Starwood's network, Marriot not only overpaid for a brand that got damaged and incurred loss of trust among its customers, but the cyber incident could result in up to $1 billion[10] in regulatory fines and litigation costs. These examples showcase the real economic and business impact that cyber breaches can incur. Investors need to take a proactive approach to cybersecurity when considering investing.

1.1 The role of the investor

Investors who provide the capital to feed innovation must guide start-ups and small and medium-sized enterprises (SMEs) in prioritizing cybersecurity. This is so important that it must be part and parcel of the innovative company strategy to ensure sustainable technology and to take full advantage of the opportunities that digitalization presents. The challenge, however, is to lead the change required in company strategy and behaviour to prioritize security.

In this insight report and during the working group's engagement, the investment community is identified as being critical to securing innovation and providing much-needed leadership in driving secure and resilient innovation. In this report, investors represent two groups:

- **Late-stage financial investors**, including private equity, pension funds and other later-stage investors
- **Strategic investors**, i.e. corporate merger and acquisition (M&A) teams

In particular, we focus on those investors interested in or having already invested in technological innovation companies. This is not limited to investors looking to specifically invest in cybersecurity innovation, but in technology-driven business in general. In the age of digitalization, most companies are moving or have already moved to be driven by technology, data and automation. Even companies not considered to be in the technology field, like The Coca-Cola Company or Walmart Inc., have in recent years grown to rely on technology and decision-making based on the digital data in their daily operations. The market rewards the digital transformation of companies, consumers and clients are demanding it and relying on technology is essential to a company's ability to remain competitive. Every company that is successfully adapting to the Fourth Industrial Revolution is a technology-driven company.

The investment community, considered broadly, has a crucial role in guiding its portfolio companies towards success. Investors are also often among the first validators of an innovation and often provide the necessary capital to allow innovation to mature from design to reality. If the goal is to embed cybersecurity as early in the process as possible, investors can and should play a key role in ensuring that insecure technology does not reach the market. This will not only build consumer trust in technology, but will also help investors reap stable and reliable returns, and enable better protection of the intellectual property of start-ups and new technologies.

Better security features are increasingly rewarded by the market. Privacy and security are of ever-greater importance to consumers. Recent research by Bain & Company,[11] highlights that customers would be willing to buy more and pay more for internet of things (IoT) devices if their concerns about cybersecurity risks were addressed. The research suggests that 93% of executives would pay an average 22% more for devices with better security.

The healthcare sector is also confirming a growing demand for more secure products. After the WannaCry[12] and NotPetya[13] cyber-attacks disrupted operations and services in some hospitals, hospitals began demanding that medical device manufacturers improve the cyber defence of their internet-connected infusion pumps, biopsy imaging tables and other healthcare products. Hospitals themselves are conducting tests to detect weaknesses in specific devices, and asking manufacturers to reveal the proprietary software running the products in order to identify vulnerabilities.[14]

As society becomes more dependent on technology and data-driven decisions, cybersecurity ought to be woven into every business and investment decision. Cyber risk management and cybersecurity are complimentary elements of any successful and sustainable business strategy.

1.2 Enabling investors to address cybersecurity in innovation

In the Forum's work with the investor and technology innovator communities, three main highlights emerged with respect to prioritizing security and responsibility in innovation:

1. **Awareness and standard approach needed**

   Currently, there is a lack of cybersecurity awareness and no standard approach among investors for evaluating the cybersecurity preparedness of a target or portfolio of companies. A cybersecurity-focused culture based on cyber expertise and awareness is vital to prioritizing cybersecurity in the investment process. Including cybersecurity risk assessment in the investment process is a rather new approach. Stakeholders have consequently expressed a need for the development of a due care standard to guide investor responsibility in terms of cybersecurity. Moreover, there is an expressed desire to ensure that a due care standard tailored to investor needs take a principles-based approach to influence behavioural change rather than merely prescribe specific action to be taken.

2. **Cybersecurity due diligence**

   The communities have highlighted that cybersecurity is often not given adequate consideration in the diligence process and that cybersecurity assessments should be integrated in the diligence process to assess cyber capabilities. In this regard, the World Economic Forum together with the working group has developed a cybersecurity due diligence framework, in terms of people, processes and technology across organizational and product security categories such as governance, data protection and privacy.

3. **Incentive structure**

   Incentive structures need to be adjusted so that accountability for cybersecurity is of equal importance to time-to-market. New incentive models have to be developed to strike a balance between the time-to-market and better security.

This report provides principles and guidelines for improving security as an inherent element of investor responsibility. Cybersecurity due diligence is becoming part and parcel of investor fiduciary duty. As Bhakti Mirchandani, Managing Director, Focusing Capital on the Long Term puts it, "fiduciary duty for investors increasingly involves assessing cyber risk of target investments, monitoring and mitigating cyber risk of portfolio companies." Investors have an opportunity and a leverage to deploy investable capital on improving portfolio companies' cyber capabilities. This is as important as refining operations, product delivery and any other business activity that investors act upon to improve target company development.

To find a balance between investing in new technology and enforcing foundational security controls, investors and innovators have to speak the same language and understand each other's responsibilities with regard to security and innovation. This requires answers to two key questions:

1. What are the responsibilities of investors when it comes to cybersecurity for target companies?
2. How can investors exercise and act on these responsibilities?

The cyber principles and toolkits in this report aim to answer the two questions by offering guidance to investors on how to prioritize cybersecurity in their investment portfolio companies. This begins with assessing cybersecurity preparedness and the innovation security of a potential investment target prior to investment, and by growing the cybersecurity capabilities of an organization after the investment.

The insights and recommendations in this report were developed in collaboration with more than 20 leading academics, thinkers and senior executives. The goal is to urge investors to recognize that cybersecurity is fundamental to any sustainable investment, and that they have a key role to play in ensuring it is up to standard.

1.3 Report structure

This report contains three sections to help guide investor action on cybersecurity:

1. **Cybersecurity due care principles for investors**
   Investors, whether financial or strategic, must understand the importance of cybersecurity when investing and developing the capabilities of their investment. By evaluating the current challenges that investors encounter with regard to cybersecurity in the course of the investment journey, six principles are proposed to enable investor action in both assessing and developing the cybersecurity capabilities of their investment. Investors should accurately tailor their commitment to cybersecurity, based on their level of resources and time commitment.

2. **Cybersecurity due care principles: guiding questions**
   Each of the due care principles is accompanied by guiding questions designed to enable investor understanding. It is vital that investors monitor and develop their own cybersecurity capabilities on an ongoing basis. The questions are designed to facilitate self-assessment on the due care principles (section 2.1).

3. **Cybersecurity due diligence framework**
   Cybersecurity due care principle number two recommends that investors conduct a robust due diligence assessment of the cybersecurity capabilities of potential investments prior to investing. The Cybersecurity Due Diligence Framework contributes to an investor's overall cybersecurity programme, helping to accurately evaluate investment targets on cybersecurity and inform the investment decision (section 3).

This report is the first in a series of resources that will be published as part of the World Economic Forum initiative on incentivizing secure and responsible innovation.

2. Cybersecurity Due Care Principles and Questions for Investors

2.1 Cybersecurity due care principles and guiding questions

Each of the cybersecurity principles for investors is accompanied by questions that allow self-assessment of the investor's cybersecurity preparedness to enable a better understanding of how they can implement the principles to exercise their cybersecurity due care responsibilities.

Overarching principle: Ensure requisite cyber expertise

Adequate cybersecurity expertise is foundational and vital to exercising the cyber due care principles. Investors should ensure requisite cybersecurity expertise is available to them and their investment portfolio companies either internally or through external experts. An investor's attention to cybersecurity should extend well beyond regulatory compliance and legal obligations and include regular briefings on evolving cyber risks.

Expertise should evolve to guarantee optimal efforts to stay abreast of cybersecurity developments. Overall, investors are urged to foster a cybersecurity awareness culture as most businesses, investment targets and their key assets are either becoming digital or are already in the digital domain.

Questions:

1. Are the investors trained in cybersecurity and cyber risks? (This should include a general training of the subject to enable a foundational understanding of cybersecurity and the risk issues that it can present.)
2. Are the investors briefed on the current status of cybersecurity risks, threats and their implications for financial risks?
3. Do the investors have an understanding of cybersecurity risks and the influence to the overall portfolio risk level?
4. Have the investors involved cyber experts in the evaluation of the target companies? Do they authorize independent third-party assessments to evaluate target companies?
5. How do the investors assess and quantify cyber risk?

Principle 1: Incorporate a cyber-risk tolerance

The investor incorporates cyber-risk tolerance into their portfolio risk methodology similar to other types of risks monitored, such as financial and management risks. This cyber-risk tolerance threshold indicates the investor's risk appetite and serves as a reference when making investment decisions.

Investors often have a business or fiduciary responsibility to invest within a certain risk-tolerance threshold that they develop and monitor. Now more than ever, it is vital that an investor's portfolio or business risk tolerance includes cyber-risk. Investors should develop and maintain a cyber-risk tolerance threshold at the portfolio level on which investment decisions are based. This evaluation and quantification of the investment-risk tolerance relative to cyber risk should be conducted on a regular basis to ensure that it remains consistent with the overall investment-risk appetite. Investors should make reasonable efforts to keep abreast of current and future cyber threats, understand a portfolio's risk exposure, regulatory requirements and compliance with relevant cyber-related laws and regulations, and factor these into the cyber-risk tolerance threshold.

Questions:

1. How do the investors govern cybersecurity and manage cyber risk?
2. Is cyber risk discussed on a regular basis to allow adjustment of the overall investment risk profile?
3. Do the investors understand the context of the cybersecurity risk appetite and how it influences the overall investment portfolio risk tolerance?
4. Is cyber risk examined on an enterprise level, portfolio level or sector-wide basis?
5. What policies or evidence demonstrate that cyber risk is considered as a business risk and not perceived as a purely IT issue?
6. Is cyber risk translated into real impact and business terms like business disruption, effect on the investment portfolio company, legal compliance or reputation?
7. Does the investor receive briefings on the changes occurring in cybersecurity threats, incidents, asset and regulatory landscape that might influence the cyber-risk tolerance level?

Principle 2: Conduct cyber due diligence

The investor conducts a business-relevant cybersecurity assessment of the target company in terms of people, processes and technology, as part of the due diligence evaluation and weighs the potential cyber risks against the valuation and strategic benefits of investment.

Investors devote time and resources to a due diligence process prior to their investment decision. Since most companies have become technology-dependent, cybersecurity assessment cannot be decoupled from the traditional due diligence process. Moreover, it is critical that investors recognize that cybersecurity is not merely a technological challenge, but rather a risk that involves people, processes and technology.

A cybersecurity due diligence assessment should involve a holistic evaluation of whether cybersecurity is effectively embedded within the target company's culture, and also the importance that staff attaches to cybersecurity, the robustness of the target's cybersecurity policies and processes, and compliance with relevant cyber regulation. It is significant to note that due diligence efforts are often completed in a short time period and investors often face time pressure to take advantage of attractive investment opportunities. As a result, cybersecurity due diligence probity may need to be adjusted considering the relevance of cybersecurity to a particular investment and the time constraints of investors.

Questions:

1. Have the investors developed a rigorous cybersecurity due diligence assessment? Is it incorporated into the overall due diligence process?
2. How do the investors ensure that the cybersecurity assessment is holistic and assesses the target's people, processes and technology from a cyber risk perspective?
3. How much time do the investors devote to the cybersecurity assessment within the due diligence process? Is this adequate?
4. Do the investors adjust the extent of the cybersecurity due diligence to the time they have available to conduct this?
5. How do the cybersecurity due diligence findings factor into the investment decision and the valuation of the target?

Principle 3: Determine appropriate incentive structure

In the early stage of investment negotiations, the investor clearly defines ongoing cybersecurity expectations, benchmarks and incentives for portfolio companies within investment mandates and term sheets.

To help their investment portfolio companies prioritize cybersecurity, investors should clearly develop, define and communicate their expectations prior to closing the transaction. The investor and target company have to agree upon: 1. cybersecurity requirements 2. issues that the investors expect the target company to fix and improve upon, and 3. issues that the investors will invest in helping to fix. Moreover, investors should incorporate these incentives within term sheets or investment mandates to ensure enforceability. The specific incentives should serve one of two purposes: either incentivize security or dis-incentivize insecurity.

Examples of incentives could include tying executive compensation to certain cybersecurity benchmarks or requiring a cybersecurity audit at set time intervals. The various incentives may differ based on the cyber-risk profile of the investor, the industry in which the investment operates, the regulatory landscape and cyber maturity of the target, among others. Having these incentives in place, however, will have tangible impact on cybersecurity preparedness and enhance the importance it is afforded within portfolio companies.

Questions:

1. What, if any, cybersecurity-specific incentives are included in the investor's term sheets and investment mandates?
2. How do the incentives balance positive rewards for meeting/exceeding cybersecurity expectations with consequences for not fulfilling certain requirements?
3. How do the investors enforce and monitor adherence to the cybersecurity expectations set out in the incentive structure?
4. How are the cybersecurity incentives influencing the behaviours and priorities of the portfolio companies? Are they raising the level of significance given to cybersecurity?
5. How often are cybersecurity incentives adjusted based on investor risk profile changes, industry shifts, changes in the portfolio company's cybersecurity capabilities?

Principle 4: Secure integration and development

The investor develops and follows systematic action plans to securely integrate the investment target according to the nature of the investment. These action plans span the secure integration of people, processes and technology, as well as define the support that the investor will offer to develop the target's cybersecurity capabilities. The extent of integration differs according to the type of investor (financial vs strategic) and the motivation for the investment (Figures 1 and 2).

An investor's cybersecurity responsibility with respect to its investment does not end post investment. Investors need to continue taking an active role in monitoring and developing the cybersecurity capabilities of their portfolio companies over time. This starts with a robust strategy and action plan for integrating the investment under the parent company's umbrella. The extent and scale of integration may vary: a merger or acquisition for strategic purposes may require a complete merger of people, processes and technical systems, while a financial investment from a private equity investor may require the integration of only a few centralized systems (Figure 1 and 2). Regardless of the scale of integration, the integration strategy must incorporate cybersecurity. If not, the investor may face significant downstream cyber-risk exposure and liability.

Beyond the integration plan, the parties involved in the investment transaction must agree on the cybersecurity services that the investor will provide on an ongoing basis. For example, this could include monthly cybersecurity executive leadership calls held by the investor to check on the latest cybersecurity-related developments at the portfolio companies, industry trends, best practices and offer input on how they can continue to develop capabilities.

The support services offered by the investor may vary based on the cyber-risk profile, industry, regulatory landscape and maturity of both the investment target and investor. They will, however, allow the investor to actively engage in developing the cyber capabilities of their investment and convey the importance of cybersecurity, thereby raising the significance of cybersecurity within the portfolio companies.

Questions:

1. Have the investors established clear action plans describing the security measures that need to be in place along with deadlines for implementation?
2. What are the short- and medium-term strategic activities needed to minimize cyber risk exposure? What is left to the long term?
3. What governance structures, tools and communication mechanisms are in place to ensure that cybersecurity requirements are upheld during the integration?
4. Who on the leadership and integration teams is responsible for ensuring that cybersecurity requirements are upheld during the integration?
5. What, if any, cybersecurity support services do the investors provide to their portfolio companies?

Figure 1 – Extent and scale of integration depending on investment type

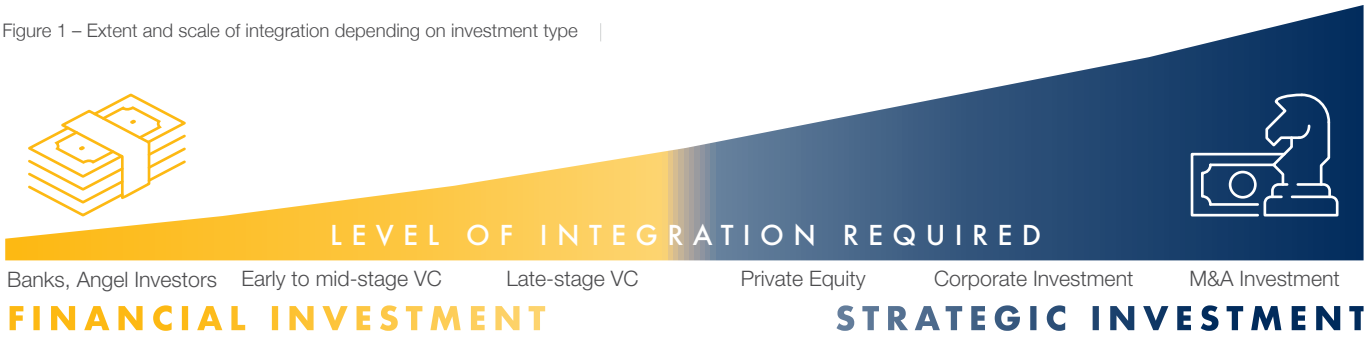
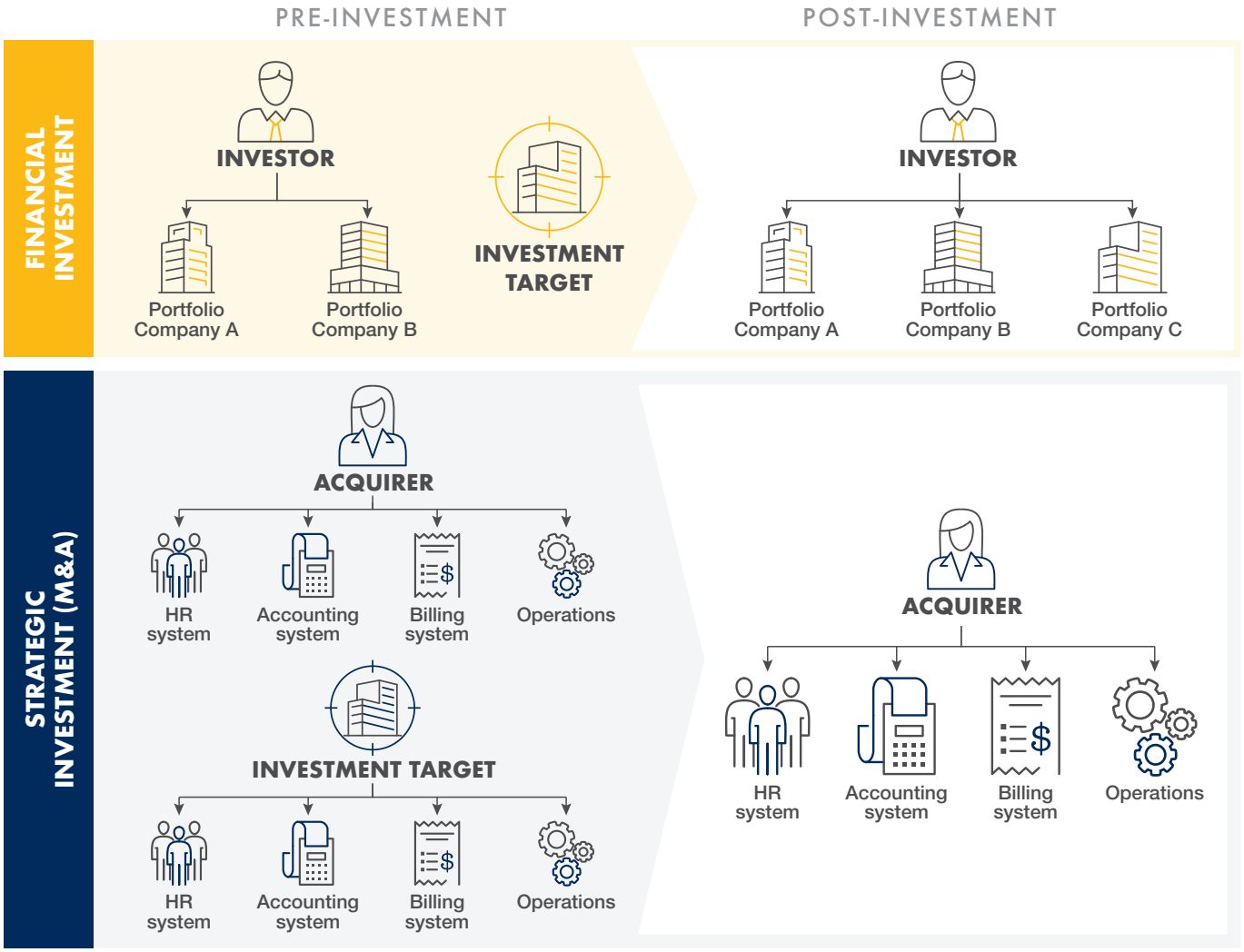


Figure 2 – Level of integration depending on the investment type



Principle 5: Regularly review and encourage collaboration

The investor reviews the cybersecurity capabilities of its portfolio companies on a regular basis. These reviews assess adherence to the cybersecurity requirements set out by the investor and serve as a basis for sharing cybersecurity challenges, best practices and lessons learned across the investor's portfolio.

Cybersecurity action plans must be regularly reviewed for their effectiveness and updated as necessary. In many instances, boards of directors conduct a third-party audit or evaluation to assess the cyber readiness of their organization. It may nevertheless be expedient for an investor to do so as well. Such reviews will provide visibility as to whether the portfolio company's cybersecurity capabilities are progressing in accordance to the requirements set out by the investor and allow the investor to accurately assess the value of a potential exit opportunity from the investment. Moreover, given that an investor will have a holistic view of the cybersecurity challenges, capabilities and best practices from their portfolio companies, they could act as a conduit to share this information within the portfolio. By doing so, the collective cybersecurity capability of the portfolio will grow and the investor can reduce the negative impact that cyber risk can have on a sale or exit of their portfolio companies.

The frequency of reviews is decisive. The investor could request reviews for policy-based matters on an annual basis, and quarterly on any financial matters.

Questions:

1. How often do the investors review the cybersecurity capabilities of the portfolio companies?
2. What mechanisms have the investors introduced to conduct these cybersecurity reviews?
3. How are the gaps found in the cybersecurity reviews communicated to the portfolio companies? How do the investors ensure that the portfolio companies have closed the identified gaps to satisfaction?
4. How, if at all, are incentive structures or investment terms changed to reflect the results of the review?
5. What mechanisms do investors have in place to share cybersecurity challenges, best practices and lessons learned with the portfolio companies? Are these effective?

2.2 Incorporating due care principles in the investment journey

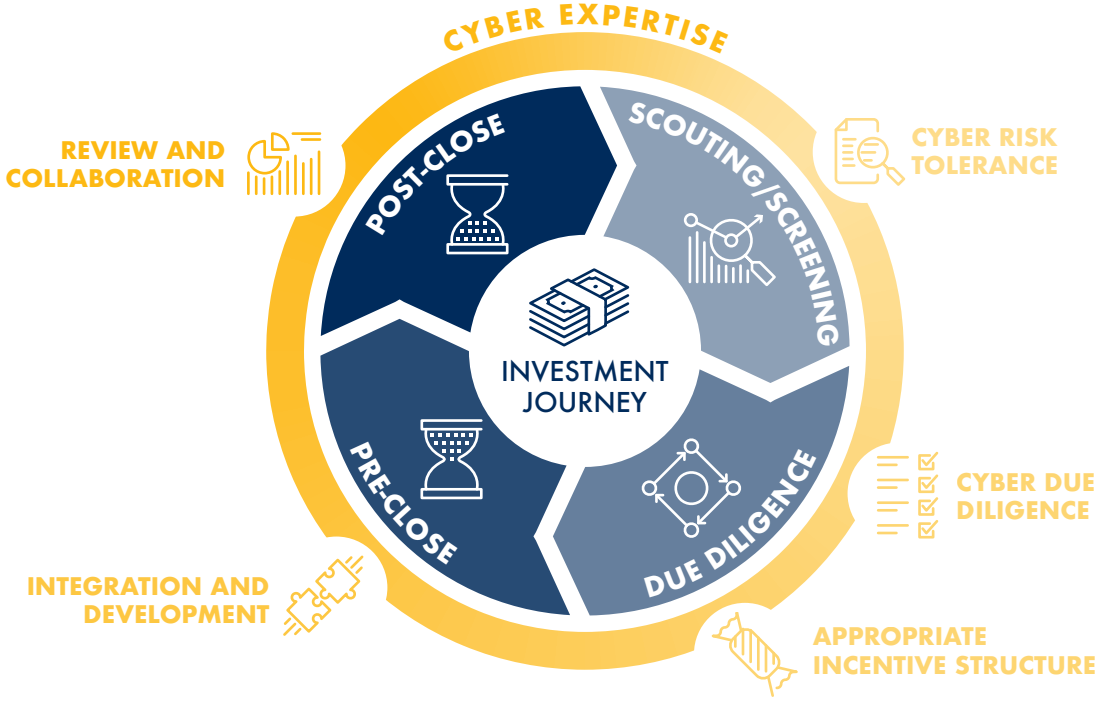


Figure 3 – Investment journey and cybersecurity due care principles

Investment in businesses presents unique opportunities and extensive value creation for the investor. Financial investors are continuously looking for the next organization to fuel with capital and achieve desired returns. Similarly, strategic investors are also looking for the next company and innovation they can either acquire or merge with to increase scale, expand business operations and ultimately create greater economic value. Regardless of the investment type, a typical investment journey can be divided into four phases:

1. **Scouting/screening**
2. **Due diligence**
3. **Pre-close**
4. **Post-close**[15]

The first two phases occur prior to the signature of the investment agreement, with the remaining two occurring after the signature and legal close of the transaction. Moreover, the ultimate goal of this journey is almost always the same – to create a larger financial return for the investor than would otherwise be possible.

When considering the cybersecurity due care responsibilities for investors through this lens (Figure 3), it becomes clear that, to facilitate investment, the principles serve a dual purpose:

1. To help improve the general state of security of innovation
2. To help investors earn more stable and reliable returns

The cybersecurity due care principles should be integrated into all phases of the investment journey.

When evaluating the cybersecurity due care principles through the lens of a typical investment journey, it is apparent that cybersecurity can and should be integrated into all phases of the process to improve the general state of security and ensure return on investment. For example, having a cyber-risk tolerance threshold in place while scouting for investment opportunities will help an investor assess whether an opportunity can fit their risk profile, thereby reducing capital availability for innovation considered not sufficiently secure while also protecting the investor from any potential financial downside.

Similarly, assessing a target company's cybersecurity capabilities in terms of due diligence efforts and on that basis informing the investment decision, valuation and any cybersecurity incentives will limit the financial downside for the investor and reduce capital availability for technologies considered insufficiently secure.

After deal closing, by monitoring and developing the cybersecurity capabilities of their investment, investors can ensure that their portfolio companies keep up with changes to the threat landscape, improvements in adversary capabilities, adjustments to business and market needs, among others. More importantly, investors play an important role in guiding their portfolio companies to step up in flagged areas identified during the cybersecurity due diligence assessment. This will ensure that the products or services the company provides have the appropriate security controls in place while increasing the value of the investment if and when it comes time for exit.

By integrating these cybersecurity due care principles throughout the investment process, investors can fulfil their responsibilities of achieving stable and reliable financial returns, understanding their portfolio's risk exposure and regulatory requirements and factors, while contributing to improving the general state of responsible and secure innovation. It is important to emphasize that the investor's responsibility is not over once the cybersecurity due diligence assessment is performed. If the investor ultimately decides to invest in the company, it is their duty to guide and lead the company to better security and improvement in areas where the portfolio company might be underperforming or presenting higher cyber-risk levels.

3. Cybersecurity Due Diligence Framework

This section presents a cybersecurity due diligence assessment framework (Figure 4) to support investors in their assessment of their target company's degree of cyber risk.

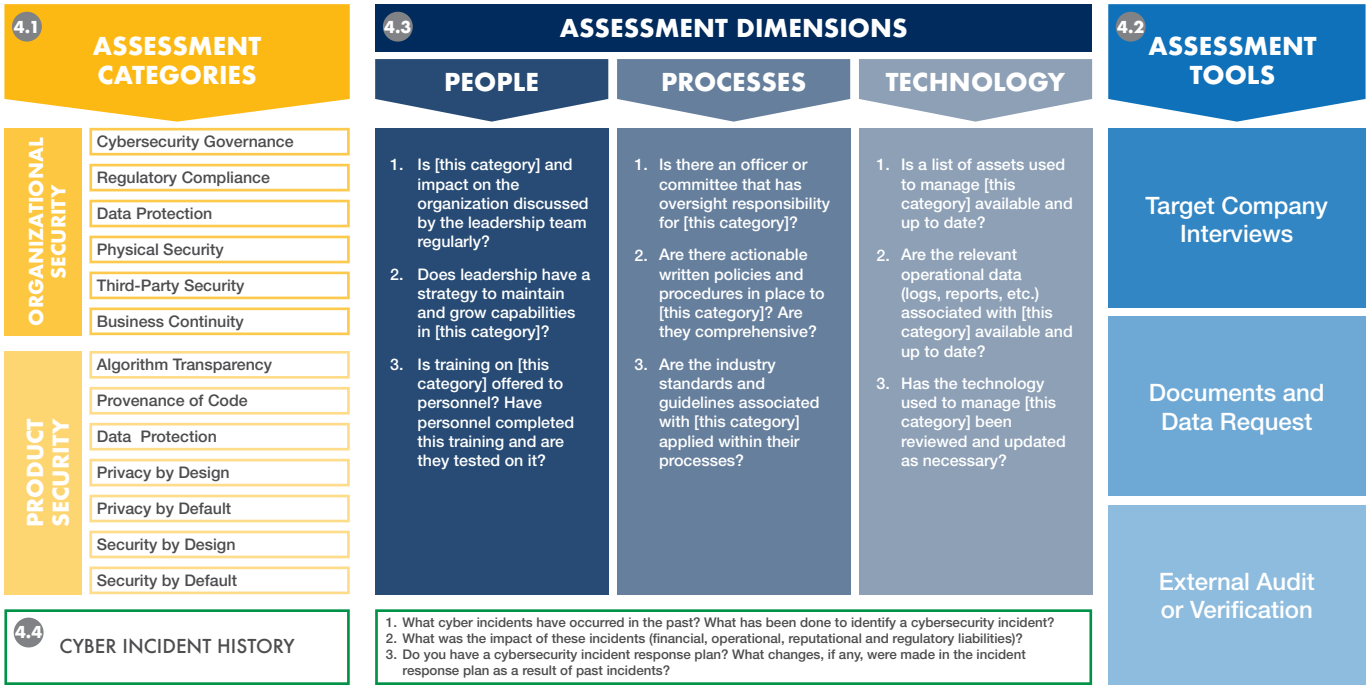


Figure 4 – Cybersecurity due diligence assessment framework at a glance with section numbers

Investing in innovation is one way to reduce the likelihood of unexpected disruption, identify "blue oceans"[16] and contribute to achieving desired returns. Whereas entrepreneurs drive innovation and experimentation, investors play an important role in helping them to grow, optimize and mature their businesses. Helping entrepreneurs to prioritize cybersecurity is one significant way in which investors can increase the likelihood of long-term success or a product's resilience in the market, thereby strengthening the brand name and consumer trust.

The World Economic Forum Centre for Cybersecurity has developed a Cybersecurity Due Diligence Assessment Framework (Figure 4), designed as a tool for the investment community for the purpose of assessing the cyber-risk profile, cyber preparedness and innovation of potential or current portfolio companies. The assessment framework can help to identify gaps in the target company's cyber risk management programme and governance. Those results allow investors to set the bar for management to improve organizational security, product security, or both. The cybersecurity assessment reveals which cyber risks are to be reduced, transferred or accepted. In this regard, the target company's cyber-risk tolerance should translate into a company-wide business strategy supported by adequate resource allocation.

Principle two of the Cybersecurity Due Care Principles (section 2.1) specifies that investors should include a cybersecurity assessment in the overall due diligence process when evaluating a target. Assessing the cybersecurity capabilities of a target company can no longer be decoupled from the due diligence process. Performing investment due diligence is not an easy task. Investment strategies vary widely, reporting results are not standardized and accessibility to key personnel and their time are limited. Still, a cyber-risk assessment contributes to the overall understanding of a target company's risk profile. Internal evaluation of the target's cyber-risk posture will measure the maximum cyber risk that the organization is able to take on and can inform

on its compatibility with the investor's cyber risk limits. It also provides the information needed to help investors prioritize risk management action, identify areas where the target company needs to improve or even remediate before an investment can proceed.

During the assessment, it is important to identify areas where cybersecurity readiness needs to improve and where investors can act by providing guidance to help prioritize cybersecurity for the purpose of reducing cyber risk. At the same time, the framework provides enhanced cybersecurity guidance and assessment categories, including common dimensions and questions for cybersecurity assessment, a risk-level scoring mechanism and practical steps for improvement. The cybersecurity assessment process can take a variety of forms, from interviewing the target company's leadership and employees to requesting third-party audits based on the assessment categories. Objective assessment by a third party might serve as a verification of interview results. More details on the process and tools can be found in section 3.2 of this report.

Improvement in cybersecurity throughout the life of an investment is necessary because a cybersecurity failure can impact the return on investment (ROI) if it is not carefully considered and addressed. Moreover, through ever-increasing connectivity, each implemented innovation that is developed without adequate security considerations increases the potential for systematic and widespread cyber-attacks. A widely used technology can constitute a single point of failure for entire industries, impact the global supply chain and influence the ever-rising interconnectedness of networks. Consequently, when investing in a technology innovation company, it is wise to evaluate not only overall organizational cybersecurity processes, but also product security, i.e. security of the software, code and algorithms.

In addition to evaluating an organization's cybersecurity, investors need an assessment tool to evaluate the security of technological innovation, or product. A product is one of the most important assets of a technology innovation company and security should be prioritized during the design and development process to ensure durability and resilience. For this reason, the Forum's Centre for Cybersecurity has developed a Cybersecurity Due Diligence Assessment Framework consisting of two parts:

1. **Organizational security**
2. **Product security**

3.1 Innovation security assessment categories

ORGANIZATIONAL SECURITY	PRODUCT SECURITY
Cybersecurity governance	Algorithmic transparency
Regulatory compliance	Provenance of code
Data protection	Data protection
Physical security	Privacy by design
Third-party security	Privacy by default
Business continuity/Disaster recovery	Security by design
CYBER INCIDENT HISTORY	Security by default

Figure 5 – Assessment categories: organizational and product security

Organizational security

Organizational security assessment must concern all internal stakeholders, including a company's executives and board of directors.

Despite its seven categories of assessment, the goal of the organizational security section is simple: to understand whether a company is implementing sufficient measures to secure its people, processes and technology, including data.

When conducting organizational security assessment, investors have to identify whether a target company fosters a cybersecurity culture. People are the most important part 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 roles and responsibilities.

If a company fails to prioritize cybersecurity readiness and awareness within their organization, there is little to no chance that they will prioritize product security. That is why the organizational security assessment should be conducted first, followed by the product security assessment.

Product security

The product security assessment applies to a narrower group of employees; the software development department and leaders responsible for product design, development and security.

To ensure that the product is developed securely, management and software development teams must be asked relevant questions. Product security is key to ensuring integrity, authentication and availability of the product and that the product continues to function correctly even under potential cybersecurity threat. Finally, it must also be developed in a manner that reduces vulnerabilities that could potentially be exploited by cyber criminals and hackers.

By prioritizing security from the very beginning of a product's development cycle, companies reduce time to market, improve agility through rapid development and rollouts, and provide an opportunity to reduce overall security risks for the product. Assessing product security throughout its development requires careful consideration of data protection; what data are collected and how data are acquired, used, stored and shared. Securing data gathered through the product is paramount to protecting user privacy and ensuring that organizational data is not compromised.

Ultimately, the purpose of developing more secure products is to reduce the attack surface by reducing the number of technological vulnerabilities and ensuring that products and systems are resilient, can be recovered quickly in case of attack.

Appendix 2 provides a more detailed explanation of all the categories, their definitions, relation to current legislation (as of June 2019) around the world and international standards. Moreover, each category is linked to a cyber incident or a financial penalty by regulators.

Regulations and frameworks in the references include, but are not limited to:

- General Data Protection Regulation (EU Law)
- NIST Special Publication 800 Series (US guidelines and recommendations)
- The Personal Data Protection Act 2012 (Singapore Law)
- The Organisation for Economic Co-operation and Development (OECD) Privacy Framework
- African Union Convention on Cyber Security and Personal Data Protection
- Asia-Pacific Economic Cooperation Privacy Framework
- The ISO/IEC 27000-series (ISO27K) international information security standards (International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC))
- Control Objectives for Information and Related Technologies (COBIT) by ISACA
- Payment Card Industry (PCI) Security Standards and Compliance

3.2 Assessment process and tools

Investors have a variety of tools with which to perform cybersecurity due diligence assessment including interviews, requesting document and data-based evidence, and obtaining external audits, like SOC1[17] and SOC2[18] reports, or third-party verification (Figure 6).

All levels of company employees must be involved in the interview process, including the leadership, product development and security teams. In conducting interviews of selected employees of a target company, investors should cover the methodology (see page 22) for each assessment category in order to understand the level and scope of cyber risk that the target company presents. The cybersecurity due diligence assessment framework recommends a list of questions that investors should ask and verify as part of the due diligence process.

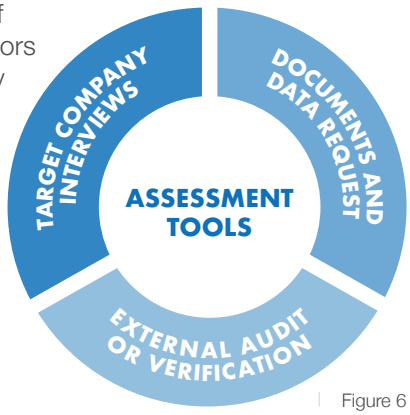


Figure 6

3.3 Assessment dimensions

Cyber risk is a business risk, albeit one with unique technical aspects.[19] As a business-wide risk, it can impact and can be impacted by all areas of the organization. As a result, both organizational and product security need to be assessed in three dimensions: People, Processes and Technology (Figure 7).

While all three dimensions are significant, the central dimension is people because they are the foundation of any security strategy and define the success of its implementation. This is why, when assessing a target company, the target's cyber-resilience assessment involves examining factors such as organization's cyber capability, commitment, the competence of its staff and user-privilege patterns.[20]

The cybersecurity due diligence assessment methodology (page 22) provides questions and potential answers rated by risk level that investors might expect during the interview process. More importantly, it guides on how the potential answers rate on a risk-level spectrum from low to high for each category (on organizational security: cybersecurity governance, regulatory compliance, data protection, physical security, third-party security, business continuity; and on product security: algorithmic transparency, provenance of code, privacy by design and default and security by design and default). While conducting interviews, investors should assess each organizational and product security category on all questions in order to get the full picture of a target company's cyber preparedness.

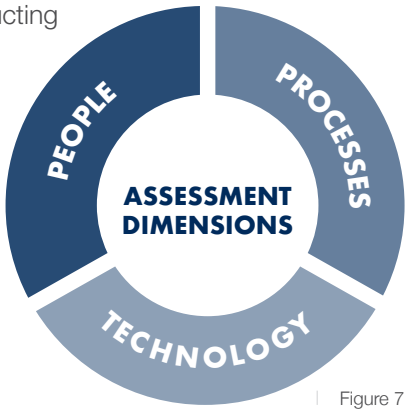


Figure 7

3.4 Cyber incident plan and history

Part of the cybersecurity due diligence assessment framework is to gather information about any known cybersecurity incident that a target company has experienced in the past. This not only prevents post-transaction surprises, but also helps to understand the target company's incident response plans and preparedness[21] in case of cyber-attack.

After Marriott International acquired Starwood in 2016 for $13.6 billion, Marriott International was surprised to find a cyber breach in Starwood's reservation system that dated back to 2014. This and similar events highlight the need to evaluate a target company's cybersecurity incident history and preparedness. Investors understand that a target's evaluation hinges not only on the strength of its cybersecurity and compliance with data privacy regulation but also on its ability to recover and continue business operations.

It is crucial to check whether a company is prepared to respond to an incident and has developed an incident-response plan that is tested regularly. As cyber threats become more sophisticated and persistent, companies must be resilient and prepared to respond to an incident.

Investors need to make sure that the target company can remediate as fast as possible and get back to business as soon as possible. No company will ever be immune to cyber-attacks but it is key that the company's resilience and preparation to recover be optimal in case an attack succeeds. The best way to assess a target's resilience is to find out whether it has created and practiced the incident response plan and whether the leadership supports it.

When gathering information about any past cyber incident and incident response plans, investors should ask to the following questions:

1. What cyber incidents have occurred at the target organization in the past? What has been done to identify a cybersecurity incident?
2. What was the impact of these incidents (in terms of financial, operational, reputational, regulatory liabilities)?
3. Does the target company have a cybersecurity incident-response plan? What changes, if any, were made in the incident-response plan as a result of past incidents? Is the plan tested regularly?

Cybersecurity Due Diligence Assessment Methodology

Rating the **risk level** of the investment target for each assessment category

	LOW	MEDIUM	HIGH
People			
Is [this category] and its impact on the organization discussed by the leadership team regularly?	[This category] has been discussed at regular intervals	[This category] has been discussed on an ad-hoc basis	[This category] has not been discussed
Does the leadership have a strategy to maintain and develop capabilities in [this category]?	Leadership has a strategy in place and an associated plan for implementation	Leadership has a strategy, but has not planned implementation	Leadership has no strategy to develop capabilities in [this category]
Is training on [this category] offered to staff? Have staff completed this training and are they tested on it?*	Training is offered and its importance is emphasized to staff. High completion percentage among personnel	Training is offered, but its importance is not emphasized. Low completion percentage among personnel	No training programmes are available for [this category]
Processes			
Does a designated officer or committee have oversight responsibility for [this category]?	Responsibility for [this category] is held by a designated officer or committee and their roles are clearly defined	Responsibility for [this category] rotates between different leaders on an ad-hoc basis	No officer or committee is responsible for [this category]
Are there actionable written policies and procedures in place to support [this category]? Are they comprehensive?	Policies and procedures associated with [this category] are in place and are comprehensive	Development of policies and procedures is in progress, but not yet comprehensive	No policies or procedures are in place to support [this category]
Are the industry standards and guidelines associated with [this category] applied in the processes?	Industry standards and guidelines have been integrated into policies and processes associated with [this category]	Industry standards and guidelines have been considered when developing policies, but not always applied	The organization is not aware of the industry standards and guidelines associated with [this category]
Technology			
Is a list of assets to manage [this category] available and up to date?	Organization has and maintains an asset list that includes the assets associated with [this category]	Organization is aware of the assets associated with managing [this category], but it is not fully up to date	Organization does not have a list of assets associated with [this category]
Are the relevant operational data (logs, reports, etc.) associated with [this category] available and up to date?	Organization collects and can provide a comprehensive set of operational data associated with [this category]	Organization collects and can provide a partial set of operational data, but it is not comprehensive	Organization does not collect or maintain the operational data associated with [this category]
Has the technology used to manage [this category] been reviewed and updated as necessary?	Technology is reviewed and updated on a regular basis	Technology is reviewed and updated, but not at an appropriate frequency	Technology is neither reviewed nor updated after implementation

*Applies to all employees in organizational security categories, applies only to development (DevOps) team in product security categories.

Cyber incident plan and history

What cyber incidents have occurred in the past? What has been done to identify a cybersecurity incident?
What was the impact of these incidents (in terms of financial, operational, reputational and regulatory liabilities)?
Do you have a cybersecurity incident response plan? What changes, if any, were made in the incident response plan as a result of past incidents?

4. Conclusion

The cyber principles and cybersecurity due diligence assessment framework recommended by the World Economic Forum aim to provide investors with the guidance and tools needed to prioritize cybersecurity in their investments. When investing in a technology company, investors needs to consider the degree of cyber risk exposure to understand how to manage and mitigate it. Investors play a critical role in leading their investment portfolio companies towards better security consideration and implementation. By proposing these tools, the World Economic Forum seeks to facilitate a useful and purposeful dialogue between investors and the leadership of target companies.

Cyber expertise comprises not only technical know-how but also cybersecurity awareness in governance and investment. The goal of the principles herein is to advance cybersecurity culture and awareness among investors. The principles and the cybersecurity due diligence assessment framework are designed for investors who want to include cybersecurity among the criteria for their investment consideration and decision. One of the main barriers to prioritizing cybersecurity is the lack of cyber expertise in the market. Yet every investor who understands the importance of cybersecurity in our technological age can ask the right questions to assess and understand a target's cybersecurity preparedness.

The investment principles and guiding questions presented in section 2.1 allow investors to self-evaluate on how well-equipped they are to prioritize cybersecurity in their investment practices. The six principles can enable investor action to lead target companies to more robust security.

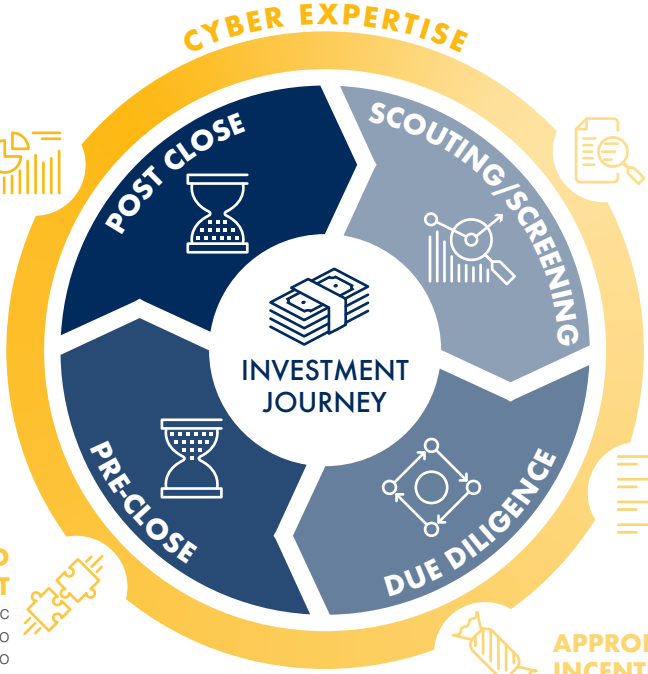
The cybersecurity due diligence assessment framework in section 3 explains in greater detail the cybersecurity due diligence assessment process. Investors should use the cybersecurity due diligence assessment framework to engage with the target company's management to evaluate and validate their cybersecurity preparedness.

The methodology (see page 22) proposes detailed questions and potential answers to assess the level of risk the answers reveal. Practically speaking, for investors, highlighting cybersecurity means exercising oversight by asking target company's leadership and management relevant questions to ensure that they have implemented cybersecurity practices in the organization and product security.

Depending on the assessment results, investors may decide to invest or not in the target company. If an investor decides to invest in the target, then the results of the cybersecurity due diligence assessment provide the investor with knowledge on the areas to be addressed in order to improve cyber resilience. If an investor does not address high-risk areas identified during the assessment, the investment is in danger to be attacked and exploited successfully. Conducting the cybersecurity assessment process is not enough; the results of the assessment should be analysed and addressed to mitigate any potential cyber risk. Cyber resilience and preparedness comprise a continuous evolving process that has to be regularly reviewed and adjusted.

Appendix 1: Cybersecurity Due Care Principles at a Glance

Adequate **expertise is vital and foundational** to execising the due care principles. Investors ensure requisite cybersecurity expertise is available either internally or through external experts throughout the investor journey



REVIEW AND COLLABORATION

Investors **review the cybersecurity capabilities** and performance of their portfolio companies on a regular basis and **facilitate collaboration** on cybersecurity across their portfolio

CYBER RISK TOLERANCE

Investors incorporate **cyber risk tolerance** at the portfolio level on which investment decisions are based

CYBER DUE DILIGENCE

Investors conduct a business relevant **cybersecurity due diligence** to assess the target company, spanning people, process, technology

INTEGRATION AND DEVELOPMENT

Investors develop a robust and systematic approach to **securely integrate** portfolio companies and **support services** to strengthen their cybersecurity capabilities

APPROPRIATE INCENTIVE STRUCTURE

In the early stage of negotiations, investors clearly define **incentives for cybersecurity and expectations**

Appendix 2: Matrix of Organizational and Product Security

	ASSESSMENT CATEGORY	DEFINITION	REGULATIONS (as of April 2019)	STANDARDS	CYBER INCIDENTS AND FINES
ORGANIZATIONAL SECURITY	Cybersecurity governance	A subset of a corporate governance that provides a strategic direction for cybersecurity activities and provides oversight on cybersecurity risk	SEC Cyber Guidance	ISO 27k Series; NIST; SOC; COBIT	Target[22]
	Regulatory compliance	Ensuring that the organization and technology fulfills all requirements prescribed by law	HIPAA; GDPR	ISO 27k Series; NIST; PCISSC; SOC & SOC2	Google fined by France[23]; Touchstone Medical Imaging[24]
	Data protection	Maintaining confidentiality, integrity and availability of all-important information	GDPR; CCPA; 23 NYCRR 500; Singapore's PDPA	ISO 27k Series; NIST; SOC	Equifax[25]; Starwood and Marriott[26]; Yahoo![27]; British Airways[28]
	Physical security	Protection of personnel, facilities, hardware, software, networks, and data from physical actions that could cause damage to an organization	NERC-CIP	ISO 27k Series; NIST; OWASP-IOT	Snowden leak[29]; Hong Kong Electoral Office[30]
	Third-party security	Protecting an organization against cybersecurity threats that originate from the supply chain, vendors or customers	23 NYCRR 500	ISO 27k Series; NIST; SOC2	Saks and Lord & Taylor[31]; MyFitnessPal[32]; Target[33]
	Business continuity/ Disaster recovery	The ability of an organization to maintain essential functions during, as well as after, a disruptive event has occurred	23 NYCRR 500	ISO 27k Series; NIST	Maersk & NotPetya[34]; NHS & WannaCry[35]
	Cyber incident plan and history	History of systems' breaches that have affected confidentiality, integrity or availability of data and operations	Gramm-Leach-Bliley Act	NIST 800-61; OECD Privacy Framework	Verizon/Yahoo [36]
PRODUCT SECURITY	Algorithm transparency	The factors that influence the decisions made by algorithms should be visible, or transparent, to the users, regulators and anyone affected by systems that employ those algorithms	GDPR; CCPA; Singapore (AI) Governance Framework		Facebook equal housing[37]
	Provenance of code	The ability to audit a software's "chain of custody" and origins, like providing a Software Bill of Materials (SBoM)		Industrial Internet Security Framework	
	Data protection	Maintaining confidentiality, integrity and availability of user information	GDPR; CCPA; 23 NYCRR 500; Singapore's PDPA; HIPPA; Asia-Pacific Privacy Framework	ISO 27k Series; NIST; SOC; AU Convention on Cyber Security	Google+[38]; Uber[39]; Equifax[40]
	Privacy by design	The prioritization of data protection throughout the whole engineering process. The software is designed with privacy as a priority	GDPR	NIST Privacy Framework; NIST SP 800-160	
	Privacy by default	The default configuration settings are the most privacy friendly settings possible without any intervention by the user	GDPR; CCPA		Google fined by France[41]
	Security by design	An approach to technology development that includes security features as a design criterion so as to minimize the number of vulnerabilities and diminish the attack surface	GDPR	NIST SP 800-160; OWASP Principles; ETSI TS	
	Security by default	The default configuration settings are the most secure settings possible without any intervention by the user	California IoT regulation; IoT Cybersecurity law	NCSC Secure by Default Principles; ETSI TS	Mirai Botnet[42]

Appendix 3: Legal References

- The European Union. The General Data Protection Regulation (2016/679). Text: https://gdpr-info.eu (link as of 21/05/19).
- The United States of America. National Institute of Standards and Technology (NIST) Special Publication 800 Series. Text: https://csrc.nist.gov/publications/sp800 (link as of 21/05/19).
- Republic of Singapore. The Personal Data Protection Act 2012 (No. 26 of 2012). Text: https://sso.agc.gov.sg/Act/PDPA2012 (link as of 21/05/19).
- International. The Organization for Economic Co-operation and Development (OECD) Privacy Framework (2013). Text: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (link as of 21/05/19).
- International. African Union Convention on Cyber Security and Personal Data Protection. (2014). Text: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (link as of 21/05/19).
- International. Asia-Pacific Economic Cooperation Privacy Framework. (2015).
- International Organization for Standardization. The ISO/IEC 27000-series (ISO27K) international information security standards. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). Text: https://www.iso.org/search.html?q=27000&hPP=10&idx=all_en&p=0&hFR[category][0]=standard (link as of 21/05/19).
- Information Systems Audit and Control Association (ISACA) Control Objectives for Information and Related Technologies (COBIT 5).
- Payment Card Industry Security Standards Council (PCISSC) PCI DSS Requiremements. 2012. Text: https://www.pcisecuritystandards.org/documents/PCI_DSS_v2_Risk_Assmt_Guidelines.pdf?agreement=true&time=1558448044647 (link as of 21/05/19).
- The United States of America. Federal Financial Institutions Examination Council (FFIEC) IT Booklets. Text: https://ithandbook.ffiec.gov/it-booklets.aspx (link as of 21/05/19).
- The United States of America. Securities and Exchange Commission. (2018). Text: https://www.sec.gov/rules/interp/2018/33-10459.pdf (link as of 21/05/19).

Contributors

Lead Author

Algirde Pipikaite	Project Lead, Governance and Policy, Centre for Cybersecurity, World Economic Forum

From the World Economic Forum

Alois Zwinggi	Member of the Managing Board, Head of the Centre for Cybersecurity, Centre for Cybersecurity
Troels Oerting	Chairman of the Advisory Board, Centre for Cybersecurity
Daniel Dobrygowski	Head of Governance and Policy, Centre for Cybersecurity
Nicholas Davis	Head of Society and Innovation, Member of the Executive Committee
Katherine Brown	Head of Sustainable and Impact Investing Initiatives
Nicole Peerless	Head of Private Investors Industry

Contributing Partners

Kelly Bissell	Senior Managing Director, Accenture Security, Accenture
Benjamin Haddad	Senior Principal, Accenture Ventures, Accenture
Tom Parker	Managing Director, Accenture Security, Accenture
Gretchen Ruck	Cybersecurity Practice Leader, AlixPartners
Jon Rigby	Director, AlixPartners
Craig Froelich	Chief Information Security Officer (CISO), Bank of America
Sounil Yu	Chief Security Scientist, Bank of America
Sawan Ruparel	Engineering Lead and Venture CTO, BCG Digital Ventures
Adam Fletcher	Chief Information Security Officer (CISO), Blackstone
Walter Bohmayr	Senior Partner and Managing Director, Boston Consulting Group
Sam Rajachudamani	Consultant, Boston Consulting Group
Katheryn Rosen	Adjunct Senior Research Scholar, School of International and Public Affairs, Columbia University
Bhakti Mirchandani	Managing Director, FCLTGlobal (Focusing Capital on the Long Term)
Elizabeth Joyce	Vice-President and Chief Information Security Officer (CISO), Hewlett Packard Enterprise

Kelly Young	Chief Information Officer (CIO), Hillspire
Adam Ghetti	Founder and Chief Executive Officer (CEO), Ionic Security
Michael Siegel	Director of Cybersecurity Center, Sloan School of Management, MIT
Martina Cheung	President, S&P Global Markets Intelligence
Marc Barrachin	Product Research & Innovation, Risk Services, S&P Global Markets Intelligence
Jim Alkove	Executive Vice-President, Security, Salesforce
Arun Singh	Senior Director, Salesforce
Lluis Pedragosa	General Partner and Chief Financial Officer (CFO), Team8
Nadav Zafrir	Co-Founder and Chief Executive Officer (CEO), Team8
Burke Norton	Principal; Co-Head, Perennial Investing, Vista Equity Partners
Anthony Dagostino	Global Head of Cyber Risk, Willis Towers Watson

Numerous other contributors supported this work by providing input, expertise and thoughtful commentary. Our thanks to: Floris van den Dool (Accenture Security), Eli Levite (Carnegie Endowment for International Peace), David Agranovich (Facebook, Inc.), Andrew McClure (ForgePoint Capital), Bruce Schneier (Harvard University), Nick Coleman (IBM), James Eckart (The Coca-Cola Company), Gundbert Scherf (McKinsey & Company, Inc.), Jan Neutze (Microsoft), Derek Vadala (Moody's Corporation), Hilary Sutcliffe (SocietyInside), Hala Furst (US Department of Homeland Security), Lars Stenqvuist (Volvo Group).

Endnotes

1. Lessig, Larry. 2006. Code, Version 2.0. New York, NY: Basic Books, p. 81-82, 120-121.
2. Eggers, Matthew and Christoper D. Roberti. 2017. Critical Infrastructure Protection, Information Sharing and Cyber Security. U.S. Chamber of Commerce. https://www.uschamber.com/issue-brief/critical-infrastructure-protection-information-sharing-and-cyber-security (link as of 13/05/19)
3. See contributors pages (29-30) for a complete list of contributing partners.
4. "The Fourth Industrial Revolution" is characterized by a range of new technologies that are fusing the physical, digital and biological worlds, impacting all disciplines, economies and industries, and even challenging ideas about what it means to be human. This term was introduced by Klaus Schwab, Founder and Executive Chairman, World Economic Forum, in his book *The Fourth Industrial Revolution*, 2016, World Economic Forum.
5. World Economic Forum. 2018. *The Global Risks Report 2018*, 13th Edition. World Economic Forum. p. 6. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf (link as of 09/05/19)
6. Greenberg, Andy. 2018. *The Untold Story of NotPetya, The Most Devastating Cyberattack in History*. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world (link as of 29/05/19)
7. Greenberg, Andy. 2018. *The Untold Story of NotPetya, The Most Devastating Cyberattack in History*. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world (link as of 11/04/19)
8. Schneier, Bruce. 2018. *Click Here to Kill Everybody: security and survival in a hyper-connected world*. New York: W.W. Norton & Company. p. 106-107.
9. Athavaley, Anjali and Shepardson, David. 2017. *Verizon, Yahoo agree to lowered $4.48 billion deal following cyberattacks*. Reuters. https://www.reuters.com/article/us-yahoo-m-a-verizon/verizon-yahoo-agree-to-lowered-4-48-billion-deal-following-cyber-attacks-idUSKBN1601EK (link as of 11/04/19)
10. Clark, Patrick. 2018. *Marriott Breach Exposes Weakness in Cyber Defenses for Hotels. Bloomberg*. https://www.bloomberg.com/news/articles/2018-12-14/marriott-cyber-breach-shows-industry-s-hospitality-to-hackers (link as of 22/04/19)
11. Ali, Saed, Bosche, Ann and Ford, Frank. 2018. *Cybersecurity Is the Key to Unlocking Demand in the Internet of Things*. Bain & Company. https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things?utm_source=linkedin_company&utm_medium=social_paid&utm_content=2199523354 (link as of 11/04/19)
12. Fluhlinger, Josh. 2018. *What is WannaCry ransomware, how does it infect and who was responsible?* CSO Online. https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html (link as of 28/05/19)
13. Palmer, Danny. 2018. *NotPetya malware attack: Chaos but not cyber warfare*. ZDNet. https://www.zdnet.com/article/notpetya-malware-attack-chaos-but-not-cyber-warfare/ (link as of 28/05/19)
14. Evans, Melanie, and Loftus, Peter. 2019. *Rattled by Cyberattacks, Hospitals Push Device Makers to Improve Security*. The Wall Street Journal. https://www.wsj.com/articles/rattled-by-cyberattacks-hospitals-push-device-makers-to-improve-security-11557662400?mod=searchresults&page=1&pos=1 (link as of 21/05/19)
15. Olyaei, Sam. 2018. *Cybersecurity Is Critical to the M&A Due Diligence Process*. Gartner.
16. Blue ocean strategy generally refers to the creation by a company of a new, uncontested market space that makes competitors irrelevant and that creates new consumer value often while decreasing costs. It was introduced by W. Chan Kim and Renée Mauborgne in their book *Blue Ocean Strategy*.

17. A Service Organization Control 1 (SOC 1) engagement is an audit of the internal controls at a service organization that have been implemented to protect client data. SOC 1 engagements are performed in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16).

18. A Service Organization Control 2 (SOC 2) report, similar to a SOC 1 report, evaluates internal controls, policies and procedures. However, the difference is that a SOC 2 reports on controls that directly relate to the security, availability, processing integrity, confidentiality and privacy at a service organization.

19. World Economic Forum. 2017. *Advancing Cyber Resilience Principles and Tools for Boards*. World Economic Forum. p. 19. http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf (link as of 09/05/19)

20. Antonucci, Domenic. 2017. *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. Wiley. p. 101.

21. Chatterjee, Chirantan and D. Daniel Sokol. 2019. *Don't Acquire a Company Until You Evaluate Its Data Security*. Harvard Business Review. https://hbr.org/2019/04/dont-acquire-a-company-until-you-evaluate-its-data-security (link as of 29/04/19)

22. Srinivasan, Suraj and Brian Kenny. 2016. *Target's Expensive Cybersecurity Mistake.* Cold Call Podcast. https://hbswk.hbs.edu/item/target-s-expensive-cybersecurity-mistake (link as of 10/05/19)

23. Hern, Alex. 2019. *Google fined record £44m by French data protection watchdog*. The Guardian. https://www.theguardian.com/technology/2019/jan/21/google-fined-record-44m-by-french-data-protection-watchdog (link as of 10/05/19)

24. Cohen, Jessica Kim. 2019. *Medical imaging company to pay $3 million HIPAA fine*. Modern Healthcare. https://www.modernhealthcare.com/technology/medical-imaging-company-pay-3-million-hipaa-fine (link as of 10/05/19)

25. Whittaker, Zack. 2018. *Equifax breach was 'entirely preventable' had it used basic security measures, says House report*. TechCrunch. https://techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report (link as of 10/05/19)

26. Whittaker, Zack. 2019. *Marriott now says 5 million unencrypted passport numbers were stolen in Starwood hotel data breach*. TechCrunch. https://techcrunch.com/2019/01/04/marriott-five-million-passport-numbers-stolen-starwood (link as of 10/05/19)

27. O'Brien, Matt. 2017. *All 3 Billion Yahoo Accounts Were Hacked*. The Associated Press. https://www.inc.com/associated-press/all-3-billion-yahoo-accounts-hacked-2013.html (link as of 10/05/19)

28. Jolly, Jasper. 2018. *British Airways: 185,000 more passengers may have had details stolen*. The Guardian. https://www.theguardian.com/business/2018/oct/25/british-airways-data-breach-185000-more-passengers-may-have-had-details-stolen (link as of 10/05/19)

29. Zetter, Kim. 2013. *Snowden Smuggled Documents From NSA on a Thumb Drive*. Wired. https://www.wired.com/2013/06/snowden-thumb-drive/ (link as of 10/05/19)

30. Chung, Kimmy and Raymond Cheng. 2017. *'Nonsense' reason for Hong Kong electoral data breach blasted*. South China Morning Post. https://www.scmp.com/news/hong-kong/politics/article/2084468/nonsense-reason-hong-kong-electoral-data-breach-blasted (link as of 10/05/19)

31. Goel, Vindu and Rachel Abrams. 2018. *Card Data Stolen From 5 Million Saks and Lord & Taylor Customers*. The New York Times. https://www.nytimes.com/2018/04/01/technology/saks-lord-taylor-credit-cards.html (link as of 10/05/19)

32. Forrest, Conner. 2018. *A breach of the Under Armour-owned app affected 150 million user accounts*. TechRepublic. https://www.techrepublic.com/article/after-massive-myfitnesspal-breach-firms-should-reconsider-mobile-fitness-programs/ (link as of 10/05/19)

33. Krebs, Brian. 2014. *Target Hackers Broke in Via HVAC Company*. Krebs on Security. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company (link as of 10/05/19)

34. Greenberg, Andy. 2018. *The Untold Story of Notpetya, The Most Devastating Cyberattack in History*. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (link as of 10/05/19)

35. Field, Matthew. 2018. *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled*. The Telegraph. https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/ (link as of 10/05/19)

36. Goel, Vindu. 2017. *Verizon Will Pay $350 Million Less for Yahoo*. The New York Times. https://www.nytimes.com/2017/02/21/technology/verizon-will-pay-350-million-less-for-yahoo.html (link as of 10/05/19)

37. Benner, Katie, Glenn Thrush and Mike Isaac. 2019. *Facebook Engages in Housing Discrimination With Its Ad Practices, U.S. Says*. The New York Times. https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html (link as of 21/05/19)

38. Newman, Lily Hay. 2018. *A New Google+ Blunder Exposed Data from 52.5 Million Users*. Wired. https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed (link as of 21/05/19)

39. Hern, Alex. 2018. *Uber fined £385,000 for data breach affecting millions of passengers*. The Guardian. https://www.theguardian.com/technology/2018/nov/27/uber-fined-385000-for-data-breach-affecting-millions-of-passengers-hacked (link as of 21/05/19)

40. Bernard, Tara Siegel, Tiffany Hsu, Nicole Perlroth and Ron Lieber. 2017. *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.* The New York Times. https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html (link as of 21/05/19)

41. Hern, Alex. 2019. *Google fined record £44m by French data protection watchdog*. The Guardian. https://www.theguardian.com/technology/2019/jan/21/google-fined-record-44m-by-french-data-protection-watchdog (link as of 10/05/19)

42. Fruhlinger, Josh. 2018. *The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet*. CSO Online. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html (link as of 10/05/19)

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