ODDO BHF
ASSET MANAGEMENT

Cybersecurity: Protecting our data!

MAY 2018

Content

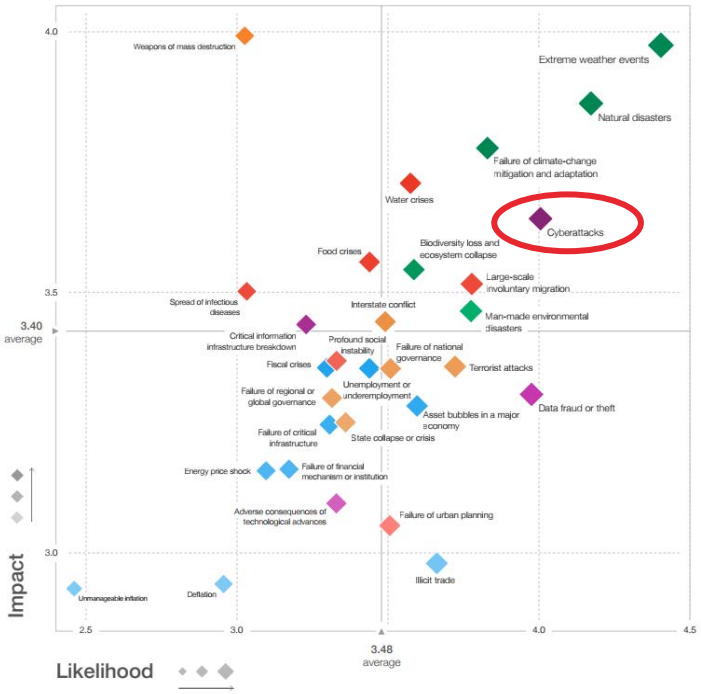
Foreword

The digitalisation of the economy in the past two decades has disrupted work and consumption habits, as well as relations between individuals and/or organisations. Companies have had to adjust to this new environment's standards of speed, mobility, connectivity and virtualisation. The digital economy now contributes more than 30% of GDP growth in developed economies and **data has become a strategic asset worth exploiting but also worth protecting.**

> *"The cost of cybercrime for the global economy could reach $8,000bn by 2022"*

With more than 3.9 billion Internet users worldwide and 8.4 billion connected objects, cybersecurity has in a few years become a major challenge for company managers, as seen in the latest survey[1] of the World Economic Forum on risk mapping for 2018.

Risk map for 2018



Source: World Economic Forum

1 http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

The study found that the cost of cybercrime for the global economy could reach $8,000bn by 2022, equivalent to almost half of the European Union's GDP. In 2017 alone there were two major cyberattacks: WannaCry (with 300,000 computers infected in 150 countries) and NotPetya (which hit companies in Ukraine, Russia, Europe and the United States). A study by Deloitte released in January 2018 found that **75% of companies surveyed said they had adopted new security measures in response to these two attacks**. So cybercrime is incurring greater and greater internal costs for companies (mainly investments in IT and human resources), as well as external costs that are hard to measure (theft of data, loss of income, business disruption and reputational risks).

Cybercriminals have many objectives, from intellectual property to financial data, but most attacks target personal data, as the exponential increase in connected objects offers an exceptionally wide field of view.

The first regulations to protect the use of personal data were adopted almost 50 years ago (in 1970 in Hesse, Germany, in 1973 in Sweden and in 1978 in France). Now more than 100 countries have passed legislation on the subject. An important development in this area is occurring in Europe in 2018, **with the General Data Protection Regulation (GDPR) entering into force on 25 May 2018** and replacing the 1995 Data Protection Directive (DPD).

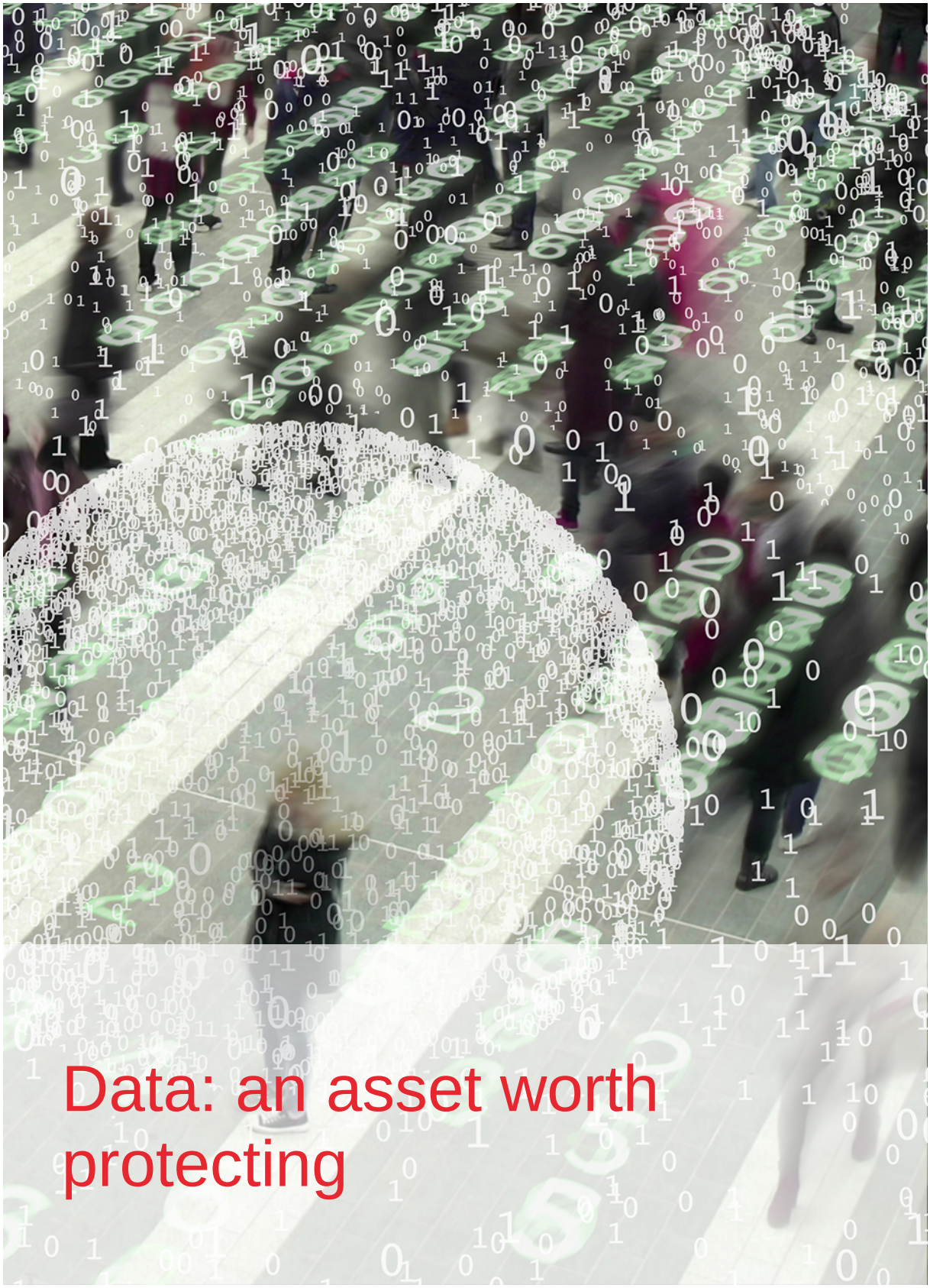
> *"The rise of cyber-risks and their impact on companies have made cybersecurity a central pillar of our dialogue approach"*

The digitalisation of the economy is clearly offering new opportunities for development in many economic sectors but also new risks, with uncertain contours and consequences that are constantly evolving.

The rise of cyber-risks, which has been made inevitable by the digital transformation of the economy, makes this an essential component in the financial and extra-financial analysis of a company. ODDO BHF Asset Management has already included it in its ESG model and cybersecurity is now one of the recurring issues that we discuss when we engage with companies.

Nicolas Jacob

Head of ESG Research, ODDO BHF Asset Management SAS



Data: an asset worth protecting

“Data is the new oil. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals etc... to create a valuable entity that drives profitable activity; so must data be broken down, analysed for it to have value.”

Clive Humby, British mathematician and big data pioneer, 2006

In 2017, one minute on the Internet amounted to 18 million persons finding out about the weather, 3.6 million Google searches, 4.1 million videos viewed on YouTube, 527,760 photos shared on Snapchat, and 103 million spams sent worldwide[2].

New opportunities, new threats

The quantity of data compiled has been expanding at an annual pace of more than 50% over the past 10 years, which has opened up a huge field of analysis for companies throughout the value chain. This data universe, which is called “big data”, is characterised by the fact that more and more data available and collected is “non-structured”, i.e., from mobile devices, Internet forums, social media and connected objects. Today more than 90% of data from the digital universe is non-structured, which is a good illustration of big data’s multiplier effect.

“A triple challenge for companies: compiling, storing and processing data”

Knowing how to process this mass of data can be a source of added value for companies, as seen in a research note published in November 2013[3] by McKinsey, which found that a good digital strategy could have significant positive impacts on companies’ earnings within five years, averaging 20% through increased income and averaging 36% through cost optimisation and productivity gains.

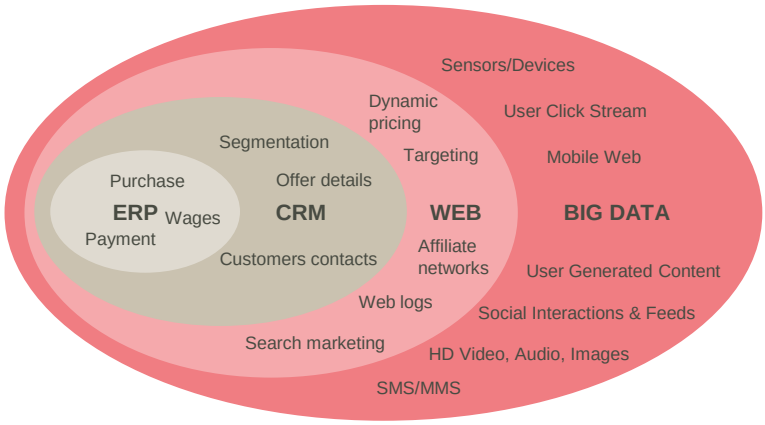
In the digital transformation process, data has thus become an essential asset for companies. But before exploiting it, they face a triple challenge: compiling, storing, and processing it.

Organisations that are able to exploit data will derive a competitive edge from it.

2 Source: Byothe.fr

3 “Finding your digital sweet spot”, McKinsey, November 2013

The growing data universe



Sources: Teradata, ODDO BHF Asset Management

Data's business value has made it an increasingly coveted asset and, hence, the target of malicious or even criminal attacks. **In 2017 alone, more than 700 million cyber-attacks occurred,** twice as many as in 2015. According to the 2018 report on data security released by Thales and 451 Research[4], 67% of 1200 IT security managers surveyed worldwide said they had already been victims of data theft.

> *"The development of the Internet of things and artificial intelligence will trigger more external cyber-attacks."*

There are many types of cyber-threats, which makes them hard to anticipate and manage for any organisation. The first line of defence is to distinguish a company's internal threats, which are still underestimated, from its external threats. Both internal and external attacks vary widely in the methods used in response and in their consequences, but, in any case, they keep growing in number with technological development. For example, the increased volume of connected objects and the development of artificial intelligence will generate a rising number of external attacks. Likewise, the development of "bring your own device" policies (allowing employees to use their personal devices to access company data) is becoming a major challenge for the security of company IT systems.

4 "2018 Thales data threat report", Thales et451 Research, Januar 2018

Cyber-threats are multi-faceted

Source: ODDO BHF Asset Management

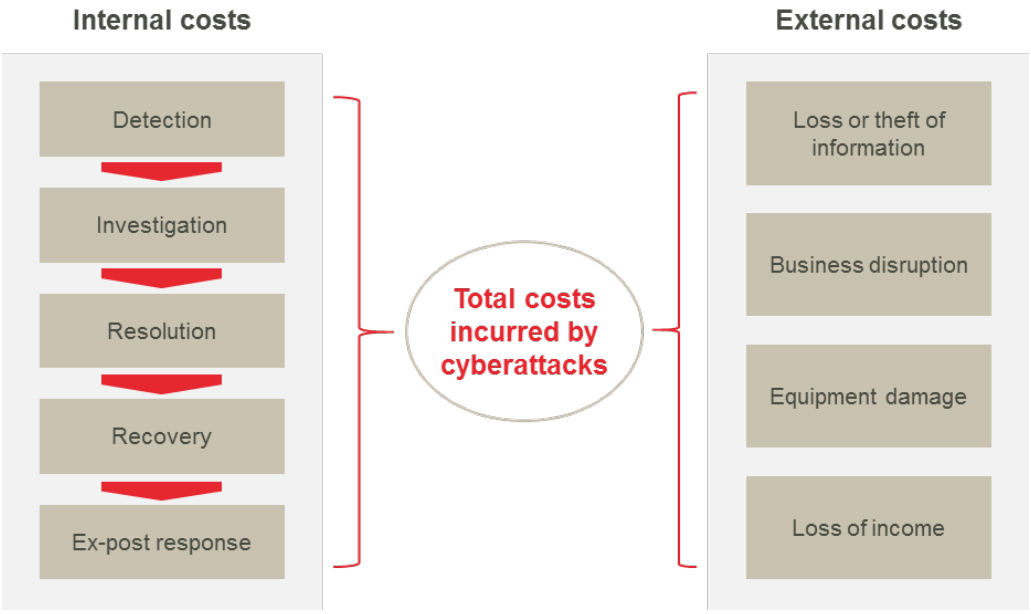
The development of mobile technologies and the Internet of things have in recent years generated a mass of **personal data that has become the favourite target of cyberattacks**. Unsurprisingly, the most heavily attacked areas are sectors focusing on the end-customer (users or consumers), such as information and communication (96% of external attacks target personal data), e-commerce (91%) and financial services (42%)[5].

5 Source: IBM X-Force Threat Intelligence Index, 2017

There is little control over impacts

The infamous cyber-attacks in 2017 (WannaCry and NotPetya) showed that the impacts no longer involved merely managing the theft or loss of data. **They are now posing more and more reputational threats to companies, costs incurred by lost income and the disruption of critical infrastructures**. NotPetya, ransomware[6], which was triggered in June 2017, first seriously disrupted the operations of Ukrainian government agencies and infrastructures before hitting many private-sector companies in the region and also companies outside Ukraine having local subsidiaries. Of those who have communicated publicly on the subject, A.P. Moeller Maersk (Denmark) and Reckitt Benckiser (United Kingdom) lost 250 and 100 million dollars, respectively, equivalent to 4 to 10% of their operating income.

Potential costs of a cyber-attack for companies



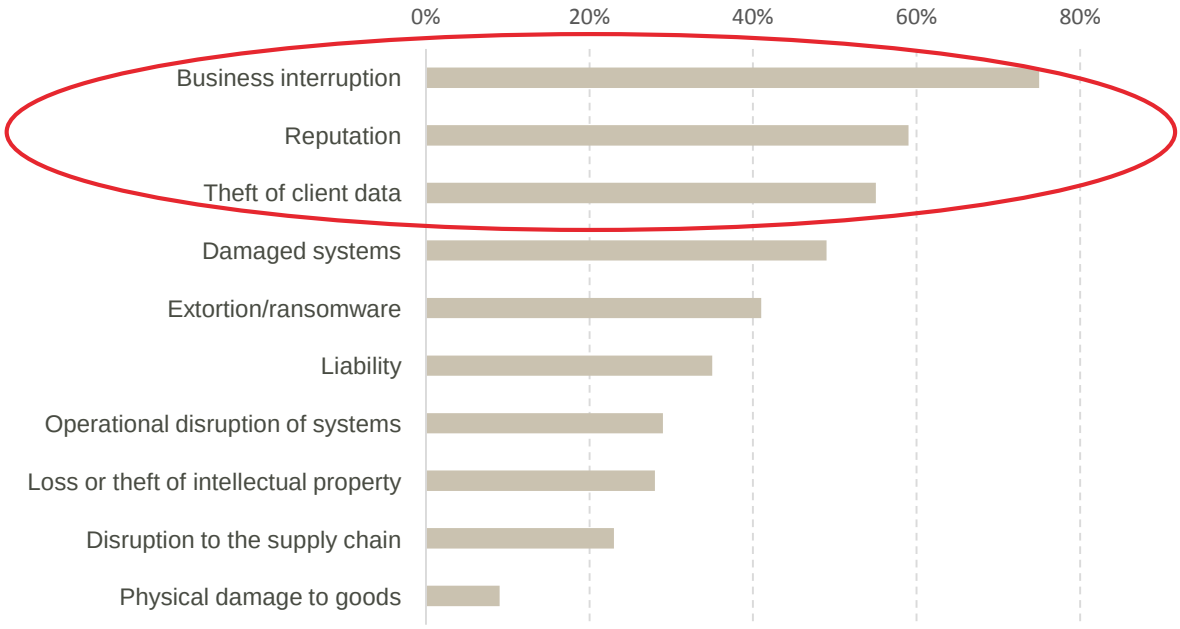
Sources: Accenture, Ponemon

This trend is playing out in companies' changing concerns. In February 2018, the research firm Marsh, in partnership with Microsoft, released the findings of a survey of 1300 decision-makers on five continents on their perception of cyber-risks, revealing that concerns had shifted clearly from internal issues (IT management, for example) towards potential consequences throughout the company's value chain (business disruption, reputational harm and theft of customer data).

6 See glossary

"The entire value chain can be affected"

The cyber-attack scenarios that companies fear the most



Source: Marsh and Microsoft Cyber perception survey, 2018

The Facebook/Cambridge Analytica affair, which was made public in March 2018[7], even raised questions about the foundations and sustainability of a business model based exclusively on compiling, storing and exploiting personal data. The affair brought to light the fact that exploiting user data without their awareness can generate a loss of trust and sustained negative impacts on a company's reputation.

> *"We have a responsibility to protect your data, and if we can't, then we don't deserve to serve you."*
>
> **Mark Zuckerberg**, founder and head of Facebook, March 2018

As things now stand, the total cost of a cyber-attack is hard to assess, especially as **intangible assets account for a growing proportion of companies' value,** which makes any attempt at a short-term estimate even more challenging.

7 Cambridge Analytica, a US strategic communications firm, siphoned the personal data of more than 80 million persons between 2014 and 2018 via Facebook.

Regulation is having a hard time keeping up

Technological disruptions continue to offer powerful new sources of growth, but very often they also create new risks that at first have been overlooked by regulators. Digitalisation is one of these disruptions and legislation takes far longer than the development of fraudulent or criminal practices.

Cyber-risks expanded exponentially in the early 2010s, alongside the acceleration in the digitalisation of the economy. **It was against this backdrop that the European Parliament in April 2016 passed a draft regulation to revise and heighten data protection mechanisms** (governed by national law in adapting the 1995 Directive). This General Data Protection Regulation (GDPR) takes effect immediately (upon its entry into force in May 2018), unlike a directive that must be transposed into national law.

The General Data Protection Regulation (GDPR)

The GDPR is the European Union's benchmark regulation for the **protection of personal data**. This set of rules replaces a previous text, dating back to 1995 (Directive 95/49/EC), which had become out-of-date in a fast-growing digital environment.

All organisations (public or private) based in the European Union or located outside the EU but managing the personal data of European residents must be in **compliance with GDPR** by 25 May 2018.

Here are its key provisions:

- **Explicit consent**: public agencies and private-sector companies must obtain users' explicit consent before compiling their personal data;
- **Right to erasure** (or the "right to be forgotten"): each EU citizen has the right to demand that all or part of his/her personal data be erased by the party in charge of processing these data, for various reasons (for example, in the event of illicit processing or revoking of consent);
- **Data portability**: all persons are entitled to recover their personal data from the entity that has compiled them, in a structured and commonly used format, in order to transmit them to another responsible party of its choice;
- **Notification of leaks**: in the event of hacking, the party responsible for processing must notify the national data protection authority, as well as the users affected;
- Public agencies (and private-sector companies with more than 250 employees) must appoint a **data protection officer**;
- **Data protection by design**: public agencies and private-sector companies must comply with data protection requirements from the initial design stage of their products, services and systems. The purpose of this provision is to **protect user data** so that it cannot be disclosed to third parties or allow such parties to know everything about users' private lives.

Moving into compliance with GDPR is a complex, time-consuming undertaking that may require major changes at companies. However, effective 25 May 2018, companies will have to prove that they are in compliance with GDPR provisions, particularly with the changes involving traceability and mapping of personal data that result from the new data protection rules.

Companies that are not in compliance risk a fine of up to €20m or 4% of their worldwide revenues.

Expert insight into cybersecurity: interview with Worldline

The digitalisation of the economy has pushed the world into the era of big data. Meanwhile, cybercrime has become more extensive and effective and is now affecting an ever-rising number of organisations and individuals. Recent events such as the Facebook/Cambridge Analytica affair show that cybersecurity has become the basis on which trust is built.

Our warm thanks to the experts at Worldline, a leader in electronic payments and transactional services, for providing us with some key and detailed insight into understanding cybersecurity.

ODDO BHF AM: As a first-tier player in electronic payments, what is your outlook on cyber-risks over the next 5 to 10 years?

Worldline: Cybersecurity is a key component of our business model and over the past few years has become the most sensitive issue in our risk map, in terms of both potential impact on our activities and probability of occurrence. This issue is discussed each month at meetings of our Executive Board regarding specific KPIs. Electronic payments is, by nature, a highly sensitive area but one that is also subject to a strict standard, the Payment Card Industry Data Security Standard (PCI DSS), which was established in 2004 by the main payment card suppliers in order to enhance control of cardholder information and reduce the fraudulent use of payment instruments. In practical terms, this involves mainly fractioning and encrypting data, so that no payment chain operator keeps too much data. Data can still be stolen but it is harder to do. Among the threats that are harder to control as they are far simpler to mount, distributed denial of service (DDoS) consists in saturating a web server and thus making it impossible to access. The attacker cuts off service to cause financial harm to a company or brand and hurt its reputation. So there is a wide range of cyber-threats, but the most dangerous ones seek to destabilise organisations, companies and public agencies.

ODDO BHF AM: Fighting new technological threats with technology seems to be the solution. How do you see cryptography developing?

Worldline: All data exchanged in electronic payments are encrypted. This is an integral part of compliance of this type of service via the use of PCI DSS, although it is applicable only once a certain revenue threshold has been met. Even so, the ongoing evolution of encryption technologies creates obstacles in working with clients, as some sectors have difficulty in adjusting. The cost of ongoing updating of technologies to integrate the most up-to-date versions of encryption technologies can become a major economic obstacle for smaller actors, particularly in e-commerce, and thus generate operating

difficulties in integration with their major partners. So the technology is effective and now quite proven, but its large-scale roll-out is being slowed by the very different economic realities and constraints from one activity sector to another.

ODDO BHF AM: Can the development of the blockchain offer some responses to cybersecurity?

Worldline: Because there is no intermediary, blockchain technology is secure by nature. As it is a chain of blocks of information fractioned and verified by the users themselves, any external attack is quite difficult, at least in private blockchains. Even so, the technology is still far from mature and there are still obstacles to developing it further, such as the lack of real time, implementation costs, and very high energy consumption (the bigger the chain, the heavier the IT resources, and the higher the energy consumption). There is still a long way to go in developing a broad, e-commerce-type app, given the size of the databases to be managed and their constant evolution. However, such technology has proven itself in closed environments. It was with this in mind, for example, that Bureau Veritas, in partnership with Worldline, in March 2018 launched the first blockchain-based food traceability label, thus giving consumers access to information at each stage of manufacturing of a product. In this case, the nature of the data is clearly defined and repetitive.

ODDO BHF AM: The entry into effect of the European Union's General Data Protection Regulation (GDPR) seems to be either underestimated by many companies, small ones in particular, or to have been completely unnoticed by most citizens. In this environment of consumer mistrust of processing of personal data, what do you see as the main gap in current legislation?

Worldline: The GDPR is impacting the value chain as a whole. Many information exchanges are currently not governed by contracts. Stepping up the level of responsibility of each stakeholder in compilation and processing of data will lead to major changes in the way of working, structuring information and carrying out inspections. For BtoC business models, there will also be the duty of ensuring the consumer's explicit consent and being able to address new rights such as the right of erasure, data portability, or objection to certain personal data processing activities. All companies will also be responsible for the processing of their employees' personal data, which will probably require a complete overhaul of many HR processes.

ODDO BHF AM: Do you believe that GDPR will help enhance cybersecurity in particular via better traceability and a responsibility that will now be placed clearly with holders of data?

Worldline: Yes, without a doubt. Keep in mind that two thirds of the obligations under GDPR involve inspection and management of risks, with the remaining third covering operating items directly linked to information systems. Switching from a compliance model to a responsibility model, with potential dissuasive fines have made this a truly cross-disciplinary issue for all organisations requiring involvement at all levels of a company. One of the foundations of this new regulation is to restore confidence in the compiling and processing of data and the means of implementation are clearly in the direction of better control of cyber-risks.

Cybersecurity, a key component in how we engage companies

Our internal ESG research model for companies has historically carved out an important role for analysing intangible assets and capital, such as human resources, innovation and organisational capital (customers, brands, suppliers and technology). In our review of organisational capital, **we include a systematic approach to companies' digital strategy, which is a source of opportunities, as well as medium-term operating risks.**

The rise of cyber-risks as a concern of company managers and their increasingly material impact on investors **have made cybersecurity a key pillar in how we engage with companies.**

A structured approach to companies' digital strategy

The use of new technologies is leading to radical changes in companies in all sectors, through the multiplication of interactions and the exceptional shortening information-processing times. A company's digital strategy can, and must, find concrete applications at both an early stage (managing costs, processing, HR and suppliers) and a later stage (marketing and distribution) of their activity.

For some companies, late-stage activities are key, and most of their efforts must focus on the customer. But for many industrial companies, the digital priority must come at an early stage, in enhancing processes in production, the supply chain, and the management of human resources.

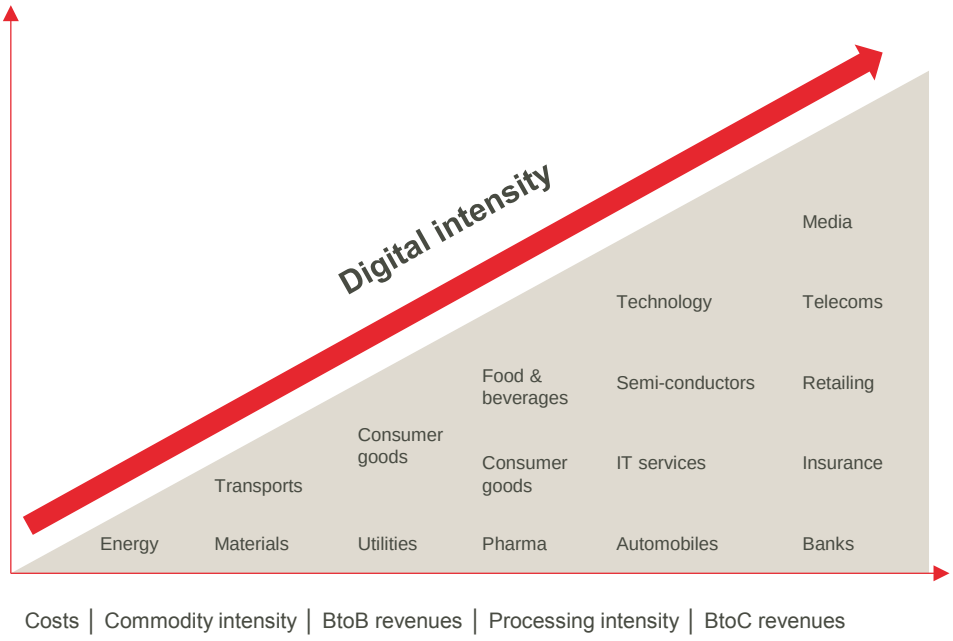
"First step: set each sector's digital intensity"

So rolling out a digital strategy depends on how each company is positioned in the value chain.

So, in our ESG research model, the first step is to weight each sector differently based on its degree of exposure to digital challenges surrounding three variables:

- Costs vs. revenues exposure,
- BtoB vs BtoC exposure,
- Commodity intensity vs. processing (HR, back-office operations, etc.).

Digital intensity of sectors



Source: ODDO BHF Asset Management

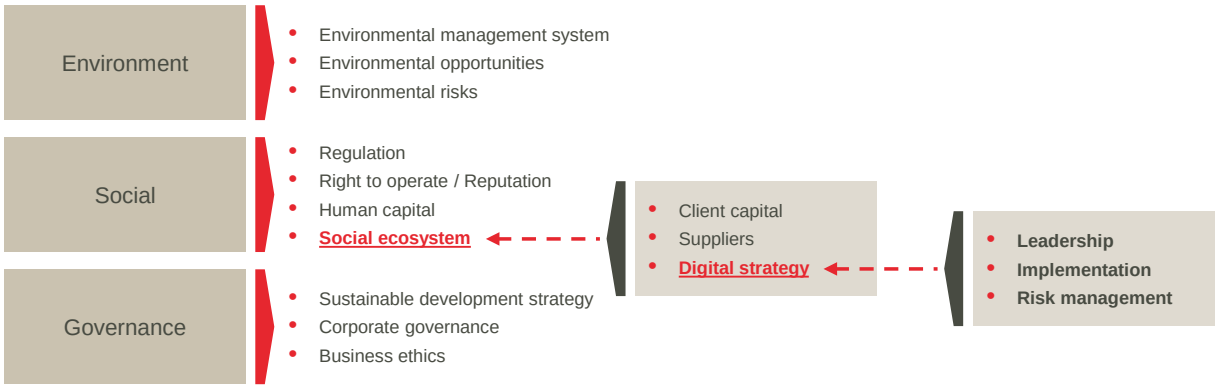
"Second step: analyse each company's digital strategy"

In a second stage, we analyse three criteria for each company:

- **Leadership**: this involves identifying who, within the company, is responsible for its digital strategy and, hence, the issue of cybersecurity (CEO, executive board, expertise of board members).
- **Implementation**: we monitor indicators such as:
  - trends in IT spending,
  - the presence of a digital team and role,
  - dedicated training for employees,
  - or the obtaining of certifications such as ISO 27001 (security of information systems) or ISO 20000 (IT production and operations).
- **Risk management**: we carry out a more qualitative analysis of the defence means implemented (roll-out of data-encryption technologies, strong authentication processes[8], cyber-insurance) and on the track-record of any incidents in data protection.

8 See glossary

Integration of digital strategy in our ESG analysis model



Source: ODDO BHF Asset Management

Cybersecurity: a source of dialogue with companies

ODDO BHF Asset Management's ESG integration policy generally gives preference to engaging with companies rather than excluding them. The digitalisation of the economy clearly offers new opportunities for development in many sectors of activity, as well as new risks whose contours and consequences are uncertain and constantly evolving.

We encourage our managers to raise this issue in their regular meetings with issuers. **The issue of cybersecurity is now discussed routinely and in accordance with the relevant sector-by-sector challenges with companies that we engage in a process of dialogue on ESG issues**.

Glossary

Botnet: contraction of the words “robot” and “network”. A botnet is a network of a large number of computers that has been taken over by a malware to serve the interests of the computer pirate that has created it. In taking control of hundreds or thousands of computers, botnets are normally used to disseminate viruses, steal personal data, or launch distributed denial of service attacks. They are currently considered to be one of the largest online threats.

Encryption: a process that makes it impossible to understand a document by any person and/or system that doesn’t have the decryption key. This is generally linked to a conditional access principle.

Personal data: any information identifying a physical person directly or indirectly (through a name, registration number, telephone number, photograph, birthdate, place of residence, fingerprints, or other means).

Hacking: the search and exploitation of fault lines in a computer system or network, often in order to obtain financial gain.

Social engineering: psychological manipulation meant to encourage individuals to disclose confidential information.

Malware: abbreviation of “malicious software”, i.e., a programme created to infect and damage a computer.

Phishing: an attempt to obtain sensitive information in by passing oneself off as a trustworthy entity in electronic communications.

Strong identification process: an identification procedure that requires a series of at least two authentication factors (or character chains).

Ransomware: a malware designed to block access to an IT system or data until payment of a sum of money, often in cryptocurrency.

References

“Guide sur le Règlement Européen relative à la protection des données personnelles”, Bird&Bird, April 2017

“Enjeux Cyber 2018: L’évolution de la menace Cyber”, Deloitte, January 2018

“Faire face aux menaces cyber”, Lloyd’s of London, September 2016

“2018 Thales data threat report”, Thales and 451 Research, January 2018

“2017 cost of cybercrime study”, Accenture and Pnemom Institute, 2017

“The Global Risks Report 2018”, World Economic Forum, January 2018

“Règlement (UE) 2016/679 du Parlement Européen et du Conseil”, Official Journal of the European Union, May 2016

About ODDO BHF Asset Management

ODDO BHF AM is part of the independent Franco-German financial group ODDO BHF that was founded in 1849.

ODDO BHF AM is an independent asset management leader in Europe. The asset management of the ODDO BHF Group comprises ODDO BHF AM SAS in France, ODDO BHF Private Equity in France and ODDO BHF AM GmbH in Germany, which together manage assets totaling close to € 61 billion.

ODDO BHF AM offers its institutional and wholesale clients a unique range of high-performance investment solutions in all main asset classes, i.e. European equities, quantitative strategies, bond and multi-asset solutions.

On a combined basis, 70% of assets under management are from institutional clients and 30% from distribution partners. The teams operate from investment centers in Dusseldorf, Frankfurt and Paris with additional locations in Luxembourg, Milan, Geneva, Stockholm and Madrid.

ODDO BHF AM puts the long-term support of its clients at the heart of its priorities. Its independence allows its teams to be responsive, flexible and innovative in order to constantly find solutions tailored to the customers’ needs.

Disclaimer

ODDO BHF AM is the asset management division of the ODDO BHF Group. It is the common brand of three legally separate asset management companies: ODDO BHF AM SAS (France), ODDO BHF Private Equity (France) and ODDO BHF AM GmbH (Germany).

This document, for market communication, has been drawn up by ODDO BHF ASSET MANAGEMENT SAS (ODDO BHF ASSET MANAGEMENT SAS) and **is exclusively dedicated to professional clients (MIFID). It may not be circulated among the public.**
The investor is informed that the strategy presents a risk of capital loss, but also many risks linked to the financial instruments/strategies in the portfolio. The value of the investment through this strategy may vary both upwards and downwards and may not be returned in full. The investment must be made in accordance with investors' investment objectives, their investment horizon and their capacity to deal with the risk arising from the transaction. ODDO BHF ASSET MANAGEMENT SAS cannot be held responsible for any direct or indirect damages resulting from the use of this document or the information contained in it. This information is provided for indicative purposes and may be modified at any moment without prior notice.
Investors are reminded that past performance is not a reliable indication of future returns and is not constant over time. Performance are presented net of fees except the potential subscription fee charged by the distributor and the local taxes. Any opinions presented in this document result from our market forecasts on the publication date. They are subject to change according to market conditions and ODDO BHF ASSET MANAGEMENT SAS shall not in any case be held contractually liable for them.

From January 3, 2018, when ODDO BHF ASSET MANAGEMENT provides investment advisory services, please note that it's always on a non-independent basis pursuant to the European Directive 2014/65/EU (so-called "MIFID II Directive"). Please also note that all recommendations made by ODDO BHF ASSET MANAGEMENT are always provided for diversification purposes.

ODDO BHF
ASSET MANAGEMENT

ODDO BHF Asset Management SAS
12 boulevard de la Madeleine
75440 Paris Cedex 09 France
am.oddo-bhf.com