ROBECOSAM
We are Sustainability Investing.

02/2016

# Cybersecurity – companies, you are under attack

**The cyber threat is omnipresent. A quick look at newspaper headlines reveals that companies from a variety of sectors such as financial services provider JP Morgan, health insurance company Anthem, and retail giant Target have all been hit by a cyber-attack within the last three years. Governments are also increasingly the targets of cyber-attacks. So it is no longer a question of if, but when an organization is attacked – and how it defends itself. Because cybersecurity breaches can have a substantial financial impact, both investors and companies must understand the cyber threat and know how to mitigate such threats. As IT security budgets grow to keep pace with increased cyber threats, IT security solutions providers are expected to benefit, in turn offering investors a range of investment opportunities.**

## Effective cybersecurity management gains complexity

As a growing number of people, organizations and devices are connected to the internet, IT systems have become more vulnerable. The large volume of data traffic and information stored result in a higher risk of major data theft or data loss incidents. And as more critical infrastructure such as power systems is controlled remotely, there is a greater chance that unauthorized people may cause a major disruption. In its Global Information Security Survey, Ernst & Young (EY) identifies five factors that have contributed to the growing complexity of cybersecurity management:[1]

1) **Change:** The pace of business development has accelerated. Shorter innovation cycles, mergers & acquisitions, quick market expansions and the introduction of new technologies require companies to move quickly.

2) **Mobility and consumerization**: With the adoption of mobile computing, organizations' boundaries are becoming blurry. IT is becoming more user-centric and mobile devices connected to the internet allow access to data from anywhere.

3) **Ecosystems:** Digitally connected entities, people and data form an ecosystem that is vulnerable to cybercrime.

4) **Cloud:** Managing and storing data in remote data centers in the cloud exposes companies to risks that do not exist in on-premise IT systems.

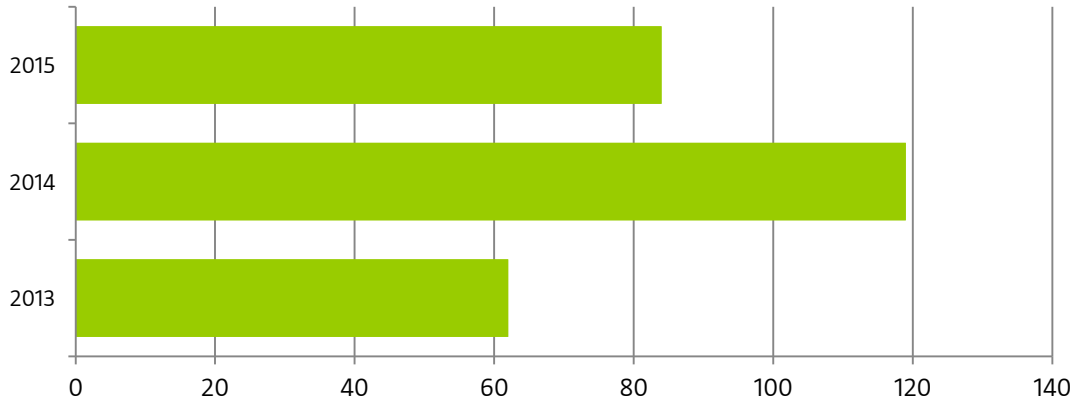
5) **Connected Infrastructure:** Infrastructure that was traditionally managed in a closed loop environment is being given IP addresses and controlled remotely. Therefore, critical infrastructures such as power generation or transportation systems are becoming potential targets of cybercriminals.

This increased complexity combined with companies' failure to keep pace with changing security requirements has resulted in a massive increase in data breach incidents over the last five years. Although it is difficult to find exact numbers of data breaches due to the lack of detection and reporting of breaches as well as the proliferation of information and communication technology, all data sources point to a growing trend of

[1] EY's Global Information Security Survey 2014

incidents comparable to the numbers outlined in Figure 1. The chart also shows that 2014 was an exceptional year with a large number of high-level data breaches, which seems to have prompted companies to better protect themselves from cyber threats. As a result, the number of severe data breaches dropped in 2015. Still, extreme data breaches took place at organizations such as Anthem, the US Office of Personnel Management, T-Mobile and Talk Talk. And with companies struggling to adapt to cyber threats quickly enough, we are likely to see more high impact cases in the future.

Figure 1: Number of severe data breaches globally*




*with a score higher than 7 out of 10

Source: Breach Level Index[2]

[2] http://breachlevelindex.com

## Prevention is costly, but the aftermath of an attack is even more expensive

According to a Ponemon Institute survey of US companies, the annualized average costs of cybercrime amounted to approximately USD 15.4 million in 2015. This represents an increase of about 21% compared to the previous year.[3] The survey also revealed that there is a positive correlation between organizational size and annualized costs for cyber-crime, which means that the costs for large publicly traded companies can be much higher.

The costs of cybercrime can impact the company in different ways. Internal costs are operational costs and relate to dealing with the cybercrime incidents and preventing new incidents. External costs include the consequences of the cyber attack such as the loss or theft of sensitive information, operations disruptions, damage to infrastructure or revenue losses due to loss of customers.

Operational costs to fix damage caused by a cyber attack such as spending for remedial actions to repair damaged infrastructure and to prevent future attacks can be substantial. Following the massive theft of its data in 2013, JP Morgan spent more than USD 250 million in FY 2014 to protect itself from the risk of future cyber attacks. To ensure effective cybersecurity, ongoing monitoring of staff and other stakeholders who have access to corporate data is paramount. In fact, employees are considered to be the second most likely source of an attack behind criminal networks, according to EY's "Global Information Security Survey 2015."

In addition to operational costs, the business impact from reputational damage, fines, and litigation costs can all have an impact on a company's long-term value. According to a study by Ponemon Institute, reputation loss, brand value and marketplace image was the most cited impact on corporate value by companies that had experienced a data breach.4 However, the full monetary impact is difficult to estimate and largely depends on how the company deals with the incident. Monetary impacts from fines are still fairly low but with new regulations proposed in different jurisdictions, fines will become more relevant for companies, especially for system-relevant sectors such as banks, telecommunications services, health care providers or utilities. For instance, according to the proposed European legislation – the General Data Protection Information Directive – companies involved in a data breach incident could be fined up to 5% of their global annual turnover or up to EUR 100 million. Furthermore, lawsuits filed by affected customers or users can result in substantial litigation costs.

Companies can use cyber insurance to mitigate the costs of cyber attacks. However, the market for cyber risk insurance is still small, with about USD 2.4 billion in premiums in 2014. Insurance represents an additional cost for the companies, especially because the premiums are priced towards the high end as insurance companies lack experience in underwriting such risks. Furthermore, damage from cyber attacks can be complex and the reputational damage is hard to quantify. Therefore, insuring the full risk of cyber attacks is almost impossible. The financial, information and communication technology and health care sectors account for the largest share of cyber-insurance premiums in the US. But as the risk for cyber-incidents becomes more relevant, the cyber insurance market is expected to grow massively over the next few years.

Despite the potentially high costs, there is no clear link between the revelation of a significant data breach and a drop in share price. For companies such as JP Morgan, eBay or Adobe Systems, stock prices did not fall on the day of the announcement, nor did they move as a result of the data breaches in the following days. However, share prices of retailers Target and Tesco – whose operating margins had been under pressure – dropped in the days following the announcement of the data breach. And in the case of Tesco, the data breach was one of the main reasons for the dismissal of its CEO. Based on these incidents, it appears that data breaches on their own – even if costly – do not change investors' sentiment if the company is otherwise doing well. But if data breaches happen when companies are experiencing general difficulties, the negative investor sentiment seems to be reinforced.

In short, data security can financially impact companies in several ways, including lower revenues, higher operating costs or higher provisions for settlements and fines, which can ultimately lower corporate values.

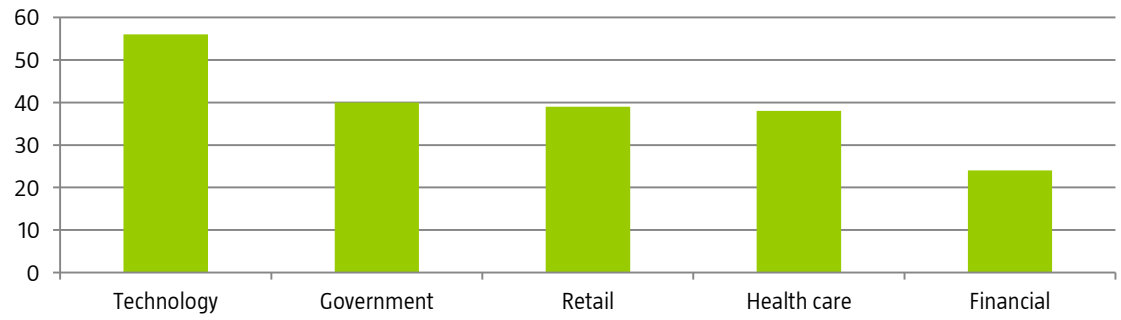
[3] Ponemon Institute: "2015 Cost of Cyber Crime Study: Global" (Ponemon Institute conducts independent research on privacy, data protection and information security policy).
[4] Ponemon Institute: 2014: A Year of Mega Breaches

## Most affected sectors

All sectors are affected by cyber attacks but the frequency of attacks, the volume of data impacted and the overall costs of data theft or loss differ. To understand which organizations are most vulnerable to attacks, it is also important to know the attackers' motivations. Although data theft and cybercrime, which seek to gain an economic or a political advantage, are currently the most dominant threats, destructive attacks are becoming more widespread as a growing network of devices – often referred to "the internet of things" – is connected to the internet. According to Symantec, cybercriminals have become much more professional over the last decade. Stolen data, malware and attack services are traded in an underground black market. Credit Card details, for instance, are traded for up to USD 20 and custom malware reaches prices of up to USD 3,500. And there is even a market for "crimeware as a service," where the entire infrastructure to run online scams can be bought.

Based on the attackers' motivations, companies that collect and store a large amount of customer/user data or organizations that have highly valuable intellectual property are all likely targets for data theft and cybercrime. This means that the technology, retail, healthcare and financial sectors are the most exposed to cyber attack, as shown in Figure 2. All of these sectors have experienced high profile data breaches; examples include financial services firm JP Morgan, health care company Anthem, e-commerce company eBay, US retailer Target or software company Adobe Systems. But other sectors such as education, telecommunication services or insurance have also experienced major incidents over the past three years. Going forward, connected cars and autonomous vehicles, for example, will expose the automotive industry to new cyber risks. Likewise, the advent of smart appliances means that industrial companies will need to invest much more in data security.

Figure 2: Number of severe data breaches by sector (2013-2015)*




*With a score higher than 7 out of 10

Source: Breach Level Index (as of 31.12.2015)[5]

[5] http://breachlevelindex.com

## RobecoSAM's approach to evaluating cyber risks

While it is clear that cyber attacks can result in major business disruptions and huge reputational damage, companies are still struggling to properly manage their cyber risks. According to EY's latest information security survey, 88% of respondents do not believe that their information security fully meets their organization's needs.[6] To mitigate the risks from data breaches or cyber attacks, companies need a strong cybersecurity strategy. Such a strategy should result in better cyber resilience, which reflects companies' ability to resist, react to and recover from potentially catastrophic cyber attacks.

RobecoSAM believes that it is important for investors to understand how companies manage cybersecurity in order to assess these cyber risks. Therefore, we ask companies about their cybersecurity strategy in our annual RobecoSAM Corporate Sustainability Assessment (CSA). Based on research from IT consultants, auditors and other investors, to determine whether companies have a comprehensive cybersecurity management strategy, we look for evidence of the elements outlined in Box 1 below.

### Elements of a company's cybersecurity strategy evaluated through the RobecoSAM Corporate Sustainability Assessment

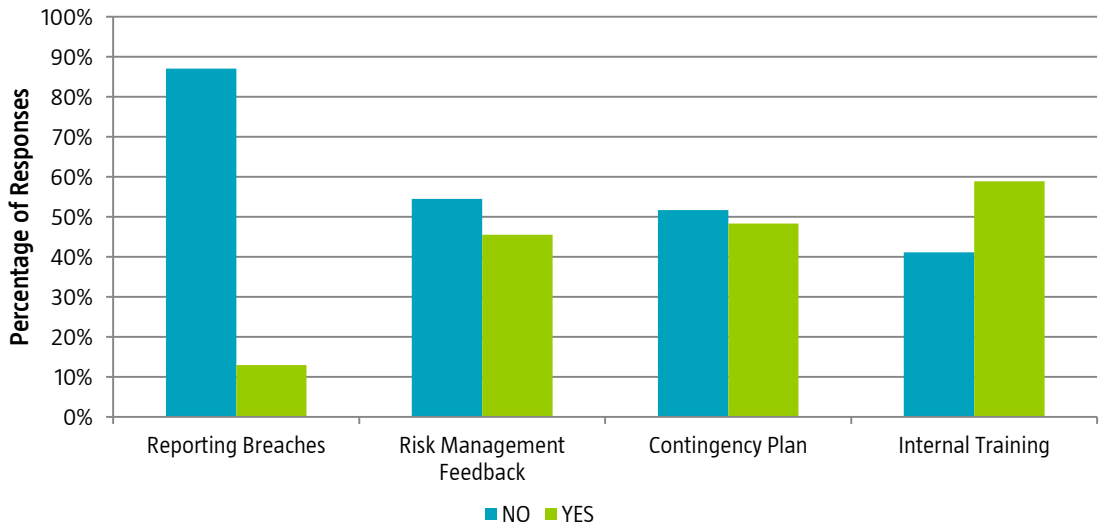
To ensure effective cybersecurity management, companies should:

- be aware of existing cyber threats through a cybersecurity assessment
- develop a comprehensive cybersecurity strategy
- ensure board-level support and clearly defined responsibilities for cybersecurity
- implement comprehensive security policies, procedures and supporting standards (e.g. ISO 27001 or NIST)
- raise employee awareness about cybersecurity and provide regular training
- establish a security operations center
- design and implement cybersecurity systems that incorporate the latest technologies

The data on cybersecurity that we collect through the annual RobecoSAM Corporate Sustainability Assessment (CSA) reveals that many companies still have major gaps in managing their cyber risks. In the 2015 assessment, we received responses from 329 companies from sectors that are highly exposed to data security risks. As shown in Figure 3, 50% of companies participating in the CSA still have not implemented any systematic contingency plans, and more than 55% have not fully integrated cyber risks into their overall corporate risk management strategy. While companies are increasingly raising internal awareness of cyber risks, with 59% of companies indicating that they do provide internal training for employees, transparency about breaches remains low, with only about 13% reporting about data breaches in the CSA.

[6] EY's Global Information Security Survey 2015

Figure 3: Data security responses in RobecoSAM Corporate Sustainability Assessment




Source: RobecoSAM

Investors should also address these issues when directly talking to company management. We do this on an ad-hoc basis in our meetings with companies, but RobecoSAM's dedicated engagement team – RobecoSAM Governance & Active Ownership – also engages with companies through a structured process. Most importantly, the insights we gain from the assessment and the dialogue with companies allow us to compare companies on their cybersecurity performance. We integrate this information into our investment cases for RobecoSAM's range of actively managed funds. For instance, US credit card company MasterCard manages its cybersecurity risks well, which is reflected in the fact that it has not experienced any major cybersecurity incidents. Thus, integrating this information into our analysis of MasterCard results in a higher fair value for the company.

## Information security: a rapidly growing market

Given the rapidly expanding cyber threats, the market for information security is growing fast. According to Gartner, an IT sector research provider, global spending for information security is expected to be more than USD 100 billion in 2015. And the market is expected to grow at a rate of about 8.7% over the next four years to reach about USD 150 billion by 2019.[7]

While traditional cybersecurity solutions such as antivirus software, traditional firewalls or email/web filters still play an important role as a first line of defense, in a world of big data and a multitude of access rights to a network, more sophisticated software solutions are required. Next-generation firewalls for instance, move beyond simply identifying threat signatures and monitor behavioral patterns of users trying to access a network. Advanced threat protection (ATP) solutions also focus on the behavior of traffic, such as abnormal traffic by unauthorized intruders. But in contrast to the next generation of firewalls, which protect the network from external threats, ATP solutions focus on threats within the networks. Another data protection solution provides encryption software, which encodes the information so that only authorized parties can decode and read it. And as the cybersecurity sector is evolving quickly, many other technologies such as big data analytics, threat intelligence or cognitive security are just about to emerge.

In addition to the various IT services companies, the main beneficiaries of increased IT security spending are companies that provide integrated security solutions in their software or hardware products and pure play IT security companies that are at the forefront of the latest technologies that focus on dynamic IT security. For integrated solution providers such as Cisco or Juniper Networks, the IT security segment is growing fast. However, it only accounts for a fraction of these firms' total revenues. For companies such as Palo Alto Networks, FireEye or CheckPoint Software, which focus exclusively on IT security solutions, growing IT security spending has a stronger impact on corporate value. But since the market already expects such IT security solutions providers to grow fast, investors should be aware of potentially overvalued companies.

[7] Gartner: Information Security, Worldwide, 2013-2019, 1Q15 Update

## Conclusion

Cyber risks have increased dramatically over the last decade. The many recent high-profile data breaches and company surveys show that a majority of companies are not up to date when it comes to protecting company assets from the current risk landscape. Therefore, **companies** must improve their cybersecurity strategies to adapt to the new ways of accessing and storing information in order to keep pace with more sophisticated attackers. For **investors,** it is important to understand the financial ramifications of cyber risks and assess which companies are best prepared to prevent data breaches, or in case intruders access the network, to react quickly to detect and neutralize the attacker. The information should then be integrated into the investment decision process. Investors should also address the topic of data security risk during their conversations with companies to raise awareness of the financial materiality of the risks. For this reason, RobecoSAM integrated questions about cybersecurity in our annual Corporate Sustainability Assessment, and engage with companies on the topic through our dedicated Governance & Active Ownership team. The information we gain from companies about their cybersecurity management is then incorporated into our investment decisions. Finally, IT security solution providers will benefit from the increased spending on IT security and therefore can be potentially interesting investment targets.

Matthias Müller, CFA
Senior Analyst

## About RobecoSAM

Founded in 1995, RobecoSAM is an investment specialist focused exclusively on Sustainability Investing. It offers asset management, indices, engagement, voting, impact analysis, sustainability assessments, and benchmarking services. Asset management capabilities cater to institutional asset owners and financial intermediaries and cover a range of ESG-integrated investments (in public and private equity), featuring a strong track record in resource efficiency theme strategies. Together with S&P Dow Jones Indices, RobecoSAM publishes the globally recognized Dow Jones Sustainability Indices (DJSI). Based on its Corporate Sustainability Assessment (CSA), an annual ESG analysis of 2,900 listed companies, RobecoSAM has compiled one of the world's most comprehensive databases of financially material sustainability information. The data of the CSA is also included in USD 89.8 billion of assets under management by Robeco.

RobecoSAM is a member of the global pure-play asset manager Robeco, which was established in 1929 and is the center of expertise for asset management within the ORIX Corporation. As a reflection of its own commitment to advocating sustainable investment practices, RobecoSAM is a signatory of the UNPRI and a member of Eurosif, ASrIA and Ceres. Approximately 130 professionals work for RobecoSAM, which is headquartered in Zurich. As of June 30, 2015, RobecoSAM had assets under management, advice and/or license in listed and private equity* of approximately USD 11.5 billion. Additionally, RobecoSAM's Governance & Active Ownership team** had USD 84 billion of assets under engagement and USD 55 billion of assets under voting.

## Disclaimer

**No warranty**: This publication is derived from sources believed to be accurate and reliable, but neither its accuracy nor completeness is guaranteed. The material and information in this publication are provided "as is" and without warranties of any kind, either expressed or implied. RobecoSAM AG and its related, affiliated and subsidiary companies disclaim all warranties, expressed or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose. Any opinions and views in this publication reflect the current judgment of the authors and may change without notice. It is each reader's responsibility to evaluate the accuracy, completeness and usefulness of any opinions, advice, services or other information provided in this publication.

**Limitation of liability**: All information contained in this publication is distributed with the understanding that the authors, publishers and distributors are not rendering legal, accounting or other professional advice or opinions on specific facts or matters and accordingly assume no liability whatsoever in connection with its use. In no event shall RobecoSAM AG and its related, affiliated and subsidiary companies be liable for any direct, indirect, special, incidental or consequential damages arising out of the use of any opinion or information expressly or implicitly contained in this publication.



**No Offer**: The information and opinions contained in this publication constitutes neither a solicitation, nor a recommendation, nor an offer to buy or sell investment instruments or other services, or to engage in any other kind of transaction. The information described in this publication is not directed to persons in any jurisdiction where the provision of such information would run counter to local laws and regulation.



RobecoSAM
Josefstrasse 218
8005 Zurich
Switzerland
T +41 44 653 10 10 - F + 41 44 653 10 80
www.robecosam.com · info@robecosam.com