November 2014

For professional investors and advisors only

Schroders
Why investors should care about data security risk

Sophie Rahm, ESG Analyst

Schroders

Contents

Executive summary

- Industry surveys as well as recent data breaches have highlighted the increasing importance of data security for companies. The annualised cost of cybercrime is thought to have risen by 26% to $11.6 million per company in 2013, according to the Ponemon Institute, an independent research group.
- The costs of data insecurity and vulnerability are real and can hit businesses in a number of ways. A data breach can lead to significant internal costs for companies, large or small, such as the need to invest in detection and recovery systems. Externally, data breaches can lead to business disruptions, information or intellectual property theft, revenue losses and erosion of customer confidence.
- More stringent regulations across the globe, particularly in the US and Europe, are likely to put data security and privacy under the spotlight. Expected regulatory changes are likely to force companies to incur additional compliance costs, as well as fines and/or litigation awards.
- According to the World Economic Forum, a robust cyber resilient environment spanning the public and private sectors could create between $10 trillion and $22 trillion in economic value between now and the end of the decade.
- The global cybersecurity solutions market is expected to grow from $64 billion in 2011 to $120 billion by 2017. Business and consumer demand for cybersecurity products increased by 15% and 10%, respectively, between 2011 and 2013. Additionally, the US cyber insurance market could reach as much as $2 billion in 2014.
- We consider the most vulnerable sectors to be Software & Services, Telecommunications Services, Retailing, Banks and Diversified Financials, although the growth and penetration of new information technologies is likely to extend the risk to all business sectors.
- A number of best-practice measures, ranging from the adoption of a company policy to strategic integration of data security risk, can help demonstrate better assimilation of these issues within a business.
- Investors can address the topic of data security risk in their conversations with companies and we propose a set of 10 cybersecurity questions.

Introduction

Stories on data breaches regularly make the headlines. Whether it be personal pictures of celebrities posted on the Internet, citizen surveillance programmes by governments or customer data being stolen on a massive scale, reports of data incidents continue to rise steadily. As noted by Symantec, an Information Technology (IT) security company, the total number of breaches in 2013 was 62% greater than in 2012, with 8 breaches exposing more than 10 million identities each. In total, over 550 million identities were exposed, putting information such as 'consumer's credit card details, birth dates, government ID numbers, home addresses, medical records, phone numbers, financial information, email addresses, passwords, and other personal information into the criminal underground'[1].

Being created at an increasing speed, data is also percolating through every aspect of our lives. This situation calls for a ramping up of data security practices, from all parties involved (individuals, governments and corporations). Data loss or theft now emerges as an important cost burden as 'more business functions move online and as more companies and consumers around the world connect to the Internet'[2].

There is little doubt that the growth of new technologies, such as mobile computing, cloud computing and virtualization, will continue and with it the exponential consumption of data. Notably, the Internet of Things, whereby people and things like smartphones, alarms, automobiles, home appliances or industrial equipment are communicating with each other, is expecting to drive cybersecurity requirements substantially[3].

The causes of data security incidents are varied; they include systems failure, infection by viruses or malicious software, theft or fraud by staff or attacks by unauthorised outsiders[4]. Traditionally, the companies whose business models focus on monetizing the storage and processing of data have been considered the most at risk. As a result, IT service providers as well as retailers, which handle large sets of customer-specific information, have been the principal victims or targets of data security breaches. This is now changing.

In this rapidly-evolving environment, the nature of the risk is manifold. Data breaches can impact negatively on the reputation of a company or customer retention may be more difficult. More strategically, intellectual property may be at jeopardy, threatening the core product proposition of a business and ultimately its economic viability. The intervention of governments, in the form of legislative requirements for data security (including privacy-related concerns) or financial sanctions, could also hit the profit line, either because there will be compliance costs to incur or fines to pay.

Several industry-wide surveys have shown that the costs of data insecurity are rising, as are the benefits of mitigating the risk effectively. This report examines how data security (or cybersecurity) risk has been increasingly placed on companies' and investors' radars.

1 Symantec, 2014. Internet Threat Report, p. 5.
2 Center for Strategic and International Studies, 2014. Net Losses: Estimating the Global Cost of Cybercrime, p. 3.
3 BAML, 2014. Safer world primer – global safety & security, p. 46.
4 DBIS, 2013. Information Security Breaches Survey, p. 11.

Materiality of data security risk

Towards greater recognition of data security risk

If the risks of data security are numerous, their materiality has been subject to debate. The acknowledged sensitivity of investors, companies, governments and civil society to data security does not always seem to align.

Looking at the share price of the stocks affected by significant data breaches in the past few years, there does not seem to be an apparent negative correlation between price and breach, i.e. the stock price does not tend to drop in the aftermath of a data incident. For instance, when eBay revealed that it had suffered a data breach on May 21, 2014, the stock finished trading unchanged on that day[5]. More significant in its scope, with 38 million users affected, the 2013 data breach at Adobe Systems left the stock unscathed. And even if stock prices may drop initially, they will ultimately stabilize around pre-breach levels, as was the case with T.J. Maxx in January 2007 when the company had a breach affecting 94 million customers.

SEC guidance on cyber security recommends that companies disclose cyber attacks or risks if that information is material to investors. The low levels of disclosure would suggest that companies do not consider these risks to be material.

Increased regulation on data security and privacy is likely to put pressure, whether it be organizational or financial, on companies and hence indirectly on investors' valuation of these companies. Such changes in the legislative environment around the globe have material implications for companies, including cost efficiencies, greater consumer trust, greater data management costs or more stringent fines.

Regulation is but a signal; the effects of data breaches and wider cyber-attacks on companies can already be measured. Although share price evolution and company self-assessment on risk materiality can be a quick test of the seriousness of data security problems, their reliability is limited: share price is but a short-term momentum indicator. Recovery can be supported by significant changes to companies' operations and companies lack the awareness that their IT systems have been breached[6].

This lack of awareness and limited appetite for transparency casts doubt over the companies' ability to be good judges of risk materiality. As noted by the Financial Times, there are 'many intrusions that companies do not report – because of trade secrecy or the commercial implications of admitting to being compromised – or the many more that simply do not know they have been infiltrated'[7].

5 Chemi, 2014.
6 Turner, 2014.
7 FT Special Report, 2014. Cyber Security, p. 3.

The costs of data insecurity

In its latest barometer on business risks, Allianz has identified cyber-crime and IT failures as a top risk, now ranking in eighth position and the biggest mover in the barometer. It shows that 'the most heightened risk awareness in 2014 is around cyber and loss of reputation issues, with risk management around the world increasingly on red alert about the threat such fast-evolving, high-tech perils pose'[8].

According to a Ponemon Institute survey, the average annualised cost of cybersecurity for responding organisations was approximately $11.6 million per year in 2013, an increase by 26% compared to last year's survey.

The costs are numerous and can hit the business in multiple ways. Internal costs relate to the recovery from a breach whilst external costs generally encompass the greater damage caused to a business in terms of operations disruption, equipment damage or revenue loss.

Theft

These main sources of direct losses from cybercrime include the theft of intellectual property (IP), financial assets, confidential business information (including customer data) as well as the money spent to secure networks in the future and the money spent on recovering from attacks. Overall, investors can be more concerned by breaches of customer data than by a theft of IP, most likely because the former tend to make the headlines as well as attract large liability settlements and fines from the regulators, ultimately hitting the profit line.

However, IP theft can also have detrimental financial consequences, albeit maybe less directly. This is due to the fact that a company's IP is very difficult to estimate. Another complication relates to the fact that hackers may well be able to steal a company's product formulations or plans and sell them on to a competitor. As noted by Center for Strategic and International Studies, a company expects a certain return on investment from its research and development programme, but 'if the research is stolen and the lead lasts only 3 months rather than a year, then the return on investment is a quarter of what it would have been in the absence of cybercrime'[9].

Fines

Increasingly, regulators add liabilities and impose fines on companies that fail to show the necessary resilience in their data security and protection system. The most noticeable trend in this respect comes from the European Union, where an updated data protection framework, if adopted would inflict strict sanctions on companies breaching data privacy laws, including a fine of up to €100m or 5% of a company's annual turnover (whichever is greater). Although some adjustments will be likely in the coming months, this reform package is expected to be completed by 2015.

8 Allianz, 2014. Allianz Risk Barometer on Business Risks, p. 4.

9 Center for Strategic and International Studies, 2014. Net Losses: Estimating the Global Cost of Cybercrime, p. 12.

There have been some recent cases where the regulator, via its data protection authority, has imposed fines on companies, either after significant data breaches or failures to comply with data regulations. Under the EU scenario, these fines would be in the order of millions (Table 1).

Table 1: Actual vs. potential fines under the EU scenario

Company	Date	Fine paid (€m)	Revenue (€m)	% revenue	EU 2% scenario (€m)	EU 5% scenario (€m)
Sony	Jan. 2013	0.29	53,800 (2012)	< 0.001%	1,076	2,690
Google	Jan. 2014	0.15	11,400 (2013)	0.001%	228	570
Thomas Cook	Jul. 2014	0.19	11,115 (2013)	0.002%	222	556

Source: Schroders

Litigation

This legislative environment intensifies the compliance risk of companies operating in the EU and represents a major burden, particularly for international companies which are generally considered less well-prepared in the area of data security and/or customer protection[10]. Additionally, costs can also soar as a result of legal proceedings, particularly in the US. Two class actions have seen Facebook and Google accept multi-million dollar lawsuit settlements in relation to the misappropriation of personal information from users:

– in August 2013, Facebook agreed to a $20 million settlement fund to compensate each class action members as well as a number of consumer protection organisations,

– in March 2014, Google proposed a $8.5 million settlement, of which $6 million would go to consumer protection organisations.

As a result, the financial impacts of data security can hit the balance sheet in a number of ways, including lower sales, higher operating costs, lower return on investment and higher provision for liabilities (settlements and fines), ultimately reducing earnings and capital available to investors.

10 MSCI ESG, Industry Report: Software & Services, August 2014, p. 10.

The benefits of risk mitigation

There are also a significant number of opportunities in this space. Cybersecurity represents a market opportunity and can deliver, either directly or indirectly, financial benefits to the firm.

The World Economic Forum highlights that countries and companies which invest in and develop cyber capabilities to instil trust in customers, citizens and investors will have a competitive edge in the digital era. The Forum adds that 'a secure, robust cyber resilience environment spanning the public and private sectors would enable business and technology innovations, such as cloud computing and mobile Internet, to create between $10 trillion and $22 trillion in economic value between now and the end of the decade'; however, should the pace and significance of cyber-attacks increase more rapidly than corresponding defence systems, a 'backlash against digitization could leave as much as $3 trillion of that value unrealised'[11].

The global cybersecurity resilience or solutions market is expected to grow from $64 billion in 2011 to $120 billion by 2017, with business and consumer demand for cybersecurity products having increased by 15% and 10%, respectively, between 2011 and 2013[12]. The pure players in data security provision systems will benefit from this trend, as will other business segments. For example, the companies that have built capability as a result of their product offering will also be in a position to exploit this growing niche and traditional information technology companies can expect to bring their internal specialty systems to the market or even provide consulting services. Additionally, given the heightened risks and their far-reaching consequences for companies, investors and consumers, we can expect the insurance sector to further develop and enhance the provision of cyber liability insurance covers (CLIC), which have been around for little over a decade. Marsh estimates that the US cyber insurance market was worth $1 billion in gross written premiums in 2013 and that it could reach as much as $2 billion in 2014[13].

From a company's perspective, one financial benefit includes a lower annualized cost of cybercrime. When security intelligence technologies are deployed by the firm, the various costs associated with data security incidents (detection, recovery, containment, ex-post response, investigation and incident management) tend to be significantly lower. Preparedness delivers cost savings.

11 World Economic Forum, 2014. Risk and Responsibility in a Hyperconnected World, p. 30.

12 BAML, 2014. Safer world primer – global safety & security, p. 46; Center for Strategic and International Studies, 2014. Net Losses: Estimating the Global Cost of Cybercrime, p. 17.

13 Marsh & McLennan, 2014. Ahead of the Curve: Understanding Emerging Risks, p. 11.

Case studies

The cases where companies have experienced data breaches are plethoric and it would be impossible to provide an exhaustive account. However, there have been some notable and well-publicised examples across a spectrum of sectors, particularly in the US, with measurable impacts on companies' operations.

Target, Home Depot

Consumer Discretionary

Profile: **Target** operates general merchandise and food discount stores in the United States. It also offers credit through its branded proprietary credit cards.

In December 2013, the US retailer Target reported a massive data breach, which involved the theft of debit and credit card data of some 40 million customers who shopped at its stores on Black Friday[14], with a further breach of personal data of 70 million customers reported in January. The breach has exposed the company to nationwide class action lawsuits from both customers and banks. It has experienced a 10% decrease in customer traffic in January 2014 compared to the previous year while its fourth-quarter earnings report showed a 5.3% fall in sales[15]. Forbes has estimated that the total cost of the breach could reach as much as $18 billion, including remediation costs, lost revenue, declining profits, lawsuits and fines[16]. This equals to approximately 24% of Target's revenues for 2013.

Profile: **Home Depot** is a home improvement retailer that sells building materials and home improvement products. It operates in the US, Canada, China and Mexico.

In September 2014, the US home improvement chain Home Depot announced that it was investigating a data breach after a security journalist found debit and credit card information from customers available for sale on the Internet. Although it is too early to speculate on potential impact on the company, it is expected that Home Depot will have to invest in its data security infrastructure as well as better and more secure card payment systems[17].

14 Black Friday marks the first day of Christmas shopping in the US, after Thanksgiving.

15 Vigeo Alert, 17 June 2014. Target Corp.

16 MSCI, 2014. Privacy and Data Security – Exploring the Data Value Chain, p. 6.

17 The card payment technology lies at the core of both companies' data breaches. There is a lack of availability of the PIN/CHIP technology in the US, where payments are still very vulnerable to fraud because they are being processed using the magnetic strip on the back of the card. Retailers have been lobbying against the PIN/CHIP due to a concern about the costs of implementation. This opposition from retailers is now likely to weaken quite rapidly given the frequency, severity and costs of attacks.

Experian

Research & Consulting Services

Profile: **Experian Plc** manages large databases that enable credit granting and monitoring as well as offers specialist analytical solutions for credit scoring, risk management and processing applications.

In 2012, Experian acquired Court Ventures, an aggregator of electronically available public records data in the USA. Court Ventures later sold the personal data of hundreds of millions of Americans (obtained via US Info Search, a subsidiary of Experian), including social security numbers, to a fraudster in Vietnam who sold on the information to thieves around the globe. The US Federal Bureau of Investigation alerted Experian in early 2013. To this date, the scope of the breach remains unclear and Experian has not communicated on the issue. It has only stated that no Experian database was accessed directly. However, this does nonetheless raise the question of Experian's due diligence process on the acquisition of Court Ventures and how its customer data could be sold on.

The company does continue to offer its expertise and data breach services to customers with its 'data breach resolution' product, and some of its services have been offered by Target customers in the aftermath of the retailer's data theft.

JPMorgan Chase

Diversified Banks

Profile: **JPMorgan Chase** provides global financial services and retail banking. It serves business enterprises, institutions and individuals.

JPMorgan Chase was amongst at least 5 banks targeted in a coordinated attack on financial institutions in the summer of 2014. Although the company declared that it had not detected any unusual fraud levels, its CEO still pledged billions to improve compliance and cybersecurity; between 2012 through the end of 2014, it will have spent an additional $2 billion on improving controls, with an annual $250 million on cybersecurity systems alone. This is partly in response to increased regulatory pressure regarding risk-weighted assets (RWA), which are used to calculate how much capital a bank needs to hold against potential losses from human error, external threats (including cyber-attacks), fraud and litigation. JPMorgan Chase's operational RWA rose to $400 billion in the second quarter of 2014, representing 24% of the company's total RWA[18].

18 JPMorgan Chase & Co, 30 June 2014, Form 10-Q, p. 76.

Company toolkit

Overall, there is a need for a more proactive approach to cybersecurity from companies. Cybersecurity has generally been considered an IT risk and so left to the responsibility of companies' IT departments. A number of measures, ranging from the adoption of a company policy to strategic integration, can help demonstrate better assimilation of these issues within the business. As companies mature their response, they will move up the ladder of data security integration and so augment their risk resilience capacity (Figure 1).

Figure 1: Building data security resilience

- Data security policy
- Data breach acknowledgement
- More transparency, public disclosure on systems and processes
- Participation in voluntary initiatives
- ISO27001 certification
- Third-party vendor audits
- Security training for all IT staff
- C-suite or executive role
- Lifecycle cost approach

Source: Schroders

At the very basic level, companies can adopt a data security **policy** (encompassing privacy issues when the company handles customer data information); this would be a de minima instrument that would help demonstrate, at the very least, that the risk is being considered.

Data breach acknowledgement could also deliver benefits, particularly with respect to customer satisfaction and loyalty. This may be in the form of greater **public recognition** and ownership of a breach (for instance, outside the materiality remit of the regulatory SEC disclosure in the United States) as well as a swift post-breach reaction. In 2011, Sony was heftily criticized for the way it managed the personal data breaches of its PlayStation and Sony Online Entertainment networks, taking almost a week to notify its customers.

Another way to promote transparency and demonstrate that the necessary tools are in place would include more corporate description of internal data security systems. Historically, companies have been reluctant to do so, claiming that this could provide hackers with an access map into their networks. An encouraging trend relates to the publication of companies' position on data privacy and security, particularly for telecommunications companies. AT&T and Verizon have both published transparency reports on the US government's demands for customer data and have committed to continuing doing so in the future[19]. In Europe, Deutsche Telekom issued a detailed report on its data privacy and security practices in 2012. Although these reports do not discuss internal systems and procedures, they do illustrate a trend of greater **transparency**, driven by customer retention concerns.

In order to develop and enhance capability, it is also recommended that companies adopt guidance principles which a growing number of governments are publishing as well as participate in voluntary initiatives on cybersecurity, thereby applying **global guidelines** but also learning from peers on how to best build in relevant and efficient responses. Some of these initiatives include the Voluntary Cybersecurity Framework, the Telecoms Industry Dialogue on Freedom of Expression and Privacy, the Cybersecurity Security and Policy Forum or the Partnership for Cyber-resilience.

A more robust and systematic method would be to seek **ISO 27001 certification**, an international standard providing requirements for an information security management system. Companies equipped with this certification have reported that it gives them a business advantage by enabling much easier due diligence compliance with customers' requests. Whilst it is no guarantee that data security breaches will not occur, it nonetheless provides reassurance and demonstrates that the company has taken the steps to embed data risk in its processes. Additionally, companies can also conduct **audits of business partners and suppliers**[20] as well as equip IT staff with greater data security skills. Recent surveys have indicated that there is both a shortage in workforce and skills: only 15% of respondents are very confident that they have the security-related skill sets needed to meet evolving threat landscapes[21].

19 http://transparency.verizon.com/international-report and http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html

20 This is particularly important for companies in the data outsourcing sector.

21 BAML, 2014. Safer world primer – global safety & security, p. 71.

Because hacks are probable and recoveries must be planned as well as executed, cybersecurity is becoming an issue for **top management**. One important indicator of whether data security risk is integrated into day-to-day business operations is the responsibility level where it sits within the organization. Ideally, this responsibility would rest in a C-suite role or at executive level. Current company performance data shows, however, that this is not common practice, although some sectors have a higher C-suite ownership of data security risk (Software and IT Services).

Ultimately, there is a need for a more integrated approach to data security, which could be achieved by conducting lifecycle risk assessment and **cost modelling**. This would factor in all the steps involved in building resilient systems and recovering from attacks. Recent research shows that, over time, a reactive approach will be more costly than proactive management, with a spike in reactive costs in the immediate aftermath of a security event. Under the proactive scenario, the company invests early on in security solutions and thus benefits from greater trust from its customer base, gaining market share and possibly being able to apply higher prices than peers[23].

23 PwC, 2010, p. 6.

Investor toolkit

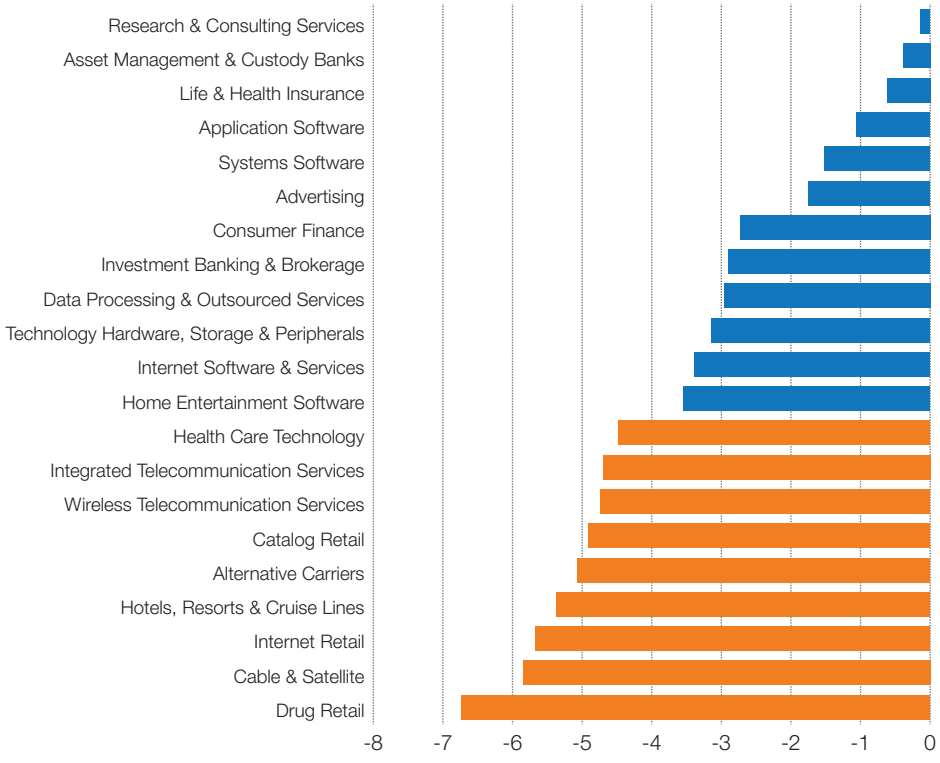
This section is designed to help investors assess companies' vulnerability to data security risk. It shows how critical sectors may fail to respond, and suggests a set of questions when engaging with companies on this issue.

We believe that data security is slowly becoming a material issue for the vast majority of business sectors in the medium- to long-term, due to the increased reliance on information technology systems to deliver both products and services. However, there are a number of sectors for which current risk exposure is relatively high, while the management response to the risk can range from adequate to lagging.

Compiling MSCI ESG data, Figure 2 shows the negative difference between risk exposure and risk management scores, thus highlighting the under-performing sectors (Figure 2).

There are a few surprises on the level of relative unpreparedness of some sectors, most notably the Information Technology ones (such as Internet Software or Data Processing & Outsourcing), for which we would expect the spread to be smaller. Telecommunication services, retailers and other customer services sector are most vulnerable. This latter observation tends to concur with our view that the penetration of data security risk tends to span beyond the technology providers. It becomes more sector-neutral as data is increasingly being commoditized.

Figure 2: Negative spread between data security risk exposure and management by sector



Source: MSCI ESG, Schroders

Additionally, investors can address the topic of data security risk in their conversations with companies to test risk resilience further. A set of 10 questions can serve as guidance during the engagement phase (Table 2).

Table 2: 10 cybersecurity questions to ask

Management Systems
Who is responsible for data security in the company? What is the responsibility level?
Does data security rest with the IT team?
Is cybersecurity a component of the overall risk management framework?
Does the company conduct any cybersecurity risk assessment?
What is the budget allocated to cybersecurity?

Operational Processes
What are the main security threats to the company?
Does the company have any cybersecurity training or awareness programmes?
Does the company use the services of a specialist third-party?
Is the company using the ISO27001 certification standard?
Is the company insured against cyber attacks?

Conclusion

Data is being created at an exponential rate and information technologies are becoming a core component of both business propositions and operations, across all sectors. In this context, the risk associated with handling and securing data, whether external or internal, becomes more obvious and tangible. Data is precious to individuals, customers and companies: when compromised it can jeopardise confidence, customer loyalty, brand reputation and profitability.

Although the impacts of data breaches can seem rather intuitive, they remain difficult to assess and evaluate, not least because it is not always known if and when a breach has occurred. For some time, even in the event of a recognised breach, an absence of stock price movement or a quick price recovery contributed to the belief that the impact was minimal, if not negligible.

The regulatory landscape is evolving quickly on the issue around the globe, with greater financial obligations being placed on companies that fail to address the risk properly. This is most notable in the European Union, where an update to the Data Privacy directive would introduce fines for an amount up to 5% of a company's global turnover, which could leave large market caps with multi-million liabilities.

There is an industry-wide effort to better understand and quantify the costs of inaction and the benefits of risk mitigation, as companies realise the value of data they hold and use. As different surveys and studies have highlighted, the cost burden of a data incident comes in different forms, at different levels: identifying and recovering from an attack or a breach demands additional investments in building more robust internal systems, while information theft, business disruption, brand damage or revenue loss resulting from the breach can impact negatively on a company's fundamentals.

Overall, there is a need for greater proactivity in data risk management from companies, which will need to demonstrate that they have operated the required shift from thinking of data security as an IT issue when, in essence, it represents a business risk.

The risk materiality as well as divide between actual performance and best practice calls for greater scrutiny from the investor community, as the robustness of a company's response needs to be better tested. The potential impacts of data security risk need to be fully understood, ideally quantified, and integrated into the investment decision-making process. Going forward, investors may want to systematically address this topic in their dialogues with companies and encourage greater recognition and management ownership of this risk in order to protect the value of their investment.

Bibliography

Allianz, 2014. Allianz Risk Barometer on Business Risks 2014.

BAML, 2014. Safer world primer – global safety & security.

Brown, 2014. "Cyber security entrepreneurs: balancing secrecy and publicity", Financial Times.

Castro, 2014. "How Much Will PRISM Cost the U.S. Cloud Computing Industry?", The Information Technology & Innovation Foundation. Available from: http://www2.itif.org/2013-cloud-computing-costs.pdf [Accessed 30 July 2014].

Chilkoti, 2014. "Community Health Systems says Chinese hackers stole patient data", Financial Times. Available from: http://www.ft.com/cms/s/0/158f1f5a-278e-11e4-be5a-00144feabdc0.html?siteedition=uk#axzz3AqXZINdp [Accessed 19 August 2014].

Center for Strategic and International Studies, 2014. Net Losses: Estimating the Global Cost of Cybercrime.

Chemi E., 2014. "Investors Couldn't Care Less About Data Breaches", Bloomberg Businessweek, Available from: http://www.businessweek.com/articles/2014-05-23/why-investors-just-dont-care-about-data-breaches [Accessed 28 July 2014].

Citi, 2012. e-Privacy & Data Protection.

Council on Cybersecurity, 2014.

Department for Business Innovation & Skills, 2013. 2013 Information Security Breaches Survey.

Deloitte, 2014. Transforming cybersecurity – New approaches for an evolving threat landscape.

European Commission, 2014. A data protection compact for Europe (speech by Viviane Reding, Vice-President of the European Commissions and EU Justice Commissioner)

Exane, 2014. Cyber wars.

FT Special Report, 2014. Cyber Security.

IRRC Institute & PWC, 2014. What investors need to know about cybersecurity: How to evaluate investment risks.

ISS, 2014. Environmental and Social Issues: Data Security, Privacy, and the Internet.

KPMG, 2014. Technology Industry Outlook – The next data-driven future.

Marsh & McLennan, 2014. Ahead of the Curve: Understanding Emerging Risks.

MSCI ESG, 2014. Industry Report: Software & Services.

MSCI ESG, 2014. Privacy and Data Security – Exploring the Data Value Chain.

New York Times, 2014. "Target cuts outlook as breach fallout lingers". Available from: http://www.nytimes.com/aponline/2014/08/20/business/ap-us-earns-target.html?_r=0 [Accessed 1 September 2014].

OECD, 2013. 'Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value', Digital Economy Papers, No. 220.

Paton, 2014. "Cyber attack takes toll on Target", Financial Times. Available from: http://www.ft.com/cms/s/0/1fcf4c82-287f-11e4-8bda-00144feabdc0.html?siteedition=uk#axzz3B0dB8GLT [Accessed 21 August 2014].

Ponemon Institute, 2013. 2013 Cost of Cyber Crime Study: United States.

PwC, 2010. Revolution or evolution? Information Security 2020.

Strohm, Engelman and Michaels, 2013. 'Cyberattacks abound yet companies tell SEC losses are few'. Available from: http://www.bloomberg.com/news/2013-04-04/cyberattacks-abound-yet-companies-tell-sec-losses-are-few.html [Accessed 30 July 2014].

Subcommittee on Counterterrorism and Intelligence, 28 June 2012. Economic Espionage: A Foreign Intelligence Threat to American Jobs and Homeland Security. Available from: http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg79843/html/CHRG-112hhrg79843.htm [Accessed 1 September 2014].

Symantec, 2014. Internet Security Threat Report, Volume 19.

The Information Technology & Innovation Foundation, 2013. How Much Will PRISM Cost the U.S. Cloud Computing Industry?

Trustwave, 2013. 2013 Global Security Report.

Turner, 2014. "Investors DO Care About Data Breaches". WAvailable from: http://blog.bitsighttech.com/investors-do-care-about-data-breaches [Accessed 28 July 2014].

Verizon, 2014. 2014 Data Breach Investigations Report.

Vigeo Alert, 17 June 2014. Target Corp.

World Economic Forum, 2012. Rethinking Personal Data: Strengthening Trust.

World Economic Forum, 2014. Risk and Responsibility in a Hyperc

www.schroders.co.uk

Schroders