Privacy versus Piracy - Security in Cyberspace Implications for ESG

Topic of the month March 2015

Introduction

More and more personal and business information worldwide is rapidly migrating into digital form on open and globally interconnected technology platforms. This poses serious risks to data security and privacy. Hardly a day goes by without news of a new cyber threat or a major data breach. Hackers, criminals and foreign governments have migrated their traditional disruptive activities, such as theft, fraud and sabotage into this increasingly interconnected world.

US whistleblower Edward Snowden's actions have put data privacy firmly on the agenda of corporates, making the topic a corporate responsibility issue. He revealed the extent of government surveillance on internet communications. Companies such as Facebook and Google had to "defend" themselves when it became apparent that they were turning user data over to the US government in response to legal orders.

Luckily, it's not all bad news. Cyberspace is constantly evolving and presenting organizations with new opportunities, as the desire of businesses to quickly adopt new technologies, such as using the Internet to open new channels and adopting cloud services, provides vast opportunity. But, it also brings unanticipated risk. The growth in the cybersecurity sector is rapid, and companies with the foresight to take advantage of these emerging trends have the potential to create value

Current state of play

Data security, also called cyber security, refers to the protection of information and data (systems) from unauthorized access, use, disclosure, disruption, modification or destruction. Privacy, on the other hand, is the appropriate use of information. It means that the data provided should only be used for the intended purpose and not disclosed to third parties without prior approval. Quite often, we hear the terms "security" and "privacy" used interchangeably. Without appropriate security programs in place you cannot ensure privacy. Conversely, you can have excellent data security practices, but fail to take the administrative measures necessary to ensure that data isn't being inappropriately shared with third-party service providers.

There are many different reasons for cybercrime, but it's not always easy to detect what motivations particular attackers have. It might be financial gain through for example fraud and identity theft. Other reasons are stealing intellectual property, making political statements or disrupting business. A common misconception is that attackers are outsiders. Unfortunately, quite frequently these are insiders: a current or former employee, service provider, authorized user of internal systems or a contractor. We are not aware of these insider incidents as most of the time they stay under the media radar and therefore we underestimate the impact of these events.

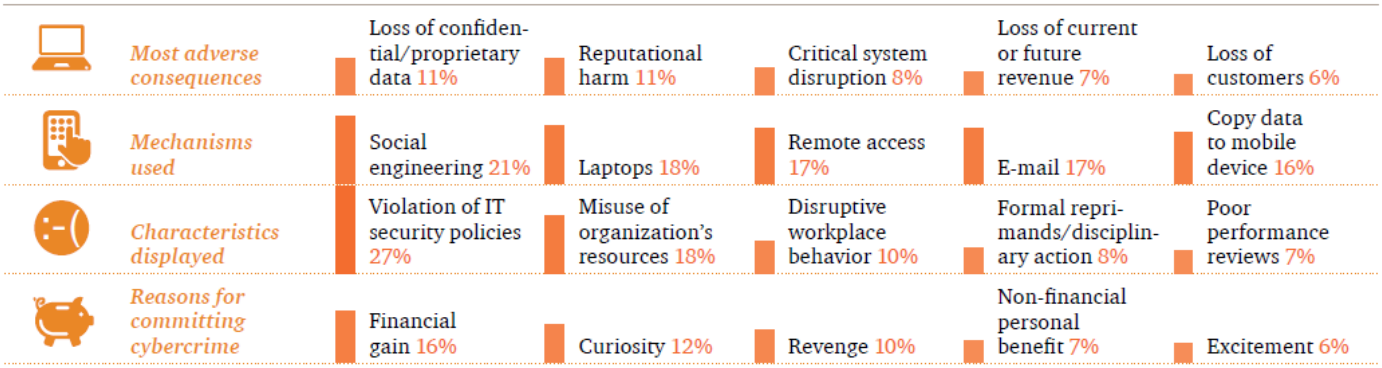

Figure 1, The causes and consequences of cybercrime committed by insiders Source: PwC 2014 US State of Cybercrime Survey

In its 2014 US State of Cybercrime Survey, PwC has found that almost one-third of respondents indicated insider crimes are more costly or damaging than incidents perpetrated by outsiders. The larger the business, the more likely it is to recognize that insider incidents can be more costly and damaging. Despite this, only 49% of all respondents have a plan for responding to insider threats. More than 500 executives of US businesses, law enforcement services, and government agencies participated in this survey. Figure 1 above shows causes and consequences of cybercrime committed by insiders.

The Center for Strategic and International Studies (CSIS) published a report in June 2014 stating that the United States, China and Germany together are estimated to have suffered $200 billion in cybercrime losses on an annual basis.

In the corporate sector, the financial and telecommunication industry are targeted the most by cyber criminals. The financial industry is exposed to a range of risks: theft of sensitive customer information, threats to business and the leak of sensitive business. Telecommunication operators control, process, transmit, receive or store electronic information and therefore are crucial to functioning of critical telecom infrastructures (e.g. in defense industry). They manage valuable information and have to comply with the legal obligations related to data protection in every country they operate.

When we look at the corporate sector, a large majority of firms are still in the developing phase of their cyber risk management capabilities. They are looking for ways to better understand which information assets need to be protected, who are their attackers and what are the most effective defense mechanisms. Today's most successful, and cyber-resilient organizations, are appointing a coordinator, such as a Director of Cybersecurity or a Chief Digital Officer (CDO), to oversee all activities in cyberspace and provide advice to the management board. One of the main questions in the data privacy area is whether companies are too-willingly passing the data to governments. Vodafone has taken the lead in this challenging debate by reporting government requests for customer personal data on a country-by-country basis (29 countries in total).

What are the next steps?

While many steps in the right direction have already been taken by the main players, there is still a long way to go. Security is a combination of prevention, detection, and response. The main challenge is that technological systems are getting more and more complex and therefore harder to secure. Simplifying procedures and reducing dependencies is needed by for example moving toward more loosely coupled systems. Moreover, there is an immediate need of executives for specific steps to improve their companies' current cyber resilience capabilities. Over time, this will also enhance companies' collaboration with partners in public and international policy, as well as community and systemic responses.

Businesses need to make sure customers trust them. Trust can make or break deals. The private and public sector need to invest more in attracting, retaining and rewarding cybersecurity talent. One of the options is for example providing opportunities to black-hat hackers (bad guys) to become white-hat hackers (good guys).

How we play this theme in an our ESG equity strategy

At ING Investment Management (soon to become NN Investment Partners) we play this theme by investing in companies whose business models are clearly linked to areas such as consumer security, content security, critical infrastructure, data encryption, enterprise security, firewalls, intrusion detection, mobile security, web security, etc. We rate cyber security as an important issue in our ESG portfolio on which companies should place special focus. As such we engage with companies across different sectors on how well they are prepared against cyber-attacks and what are their initiatives in the data security and privacy area.

Author:
Nina Hodzic
Senior ESG Specialist
ING Investment Management, Zurich

Contact:
Nelson Takes
Business Development Manager
ING Investment Management, Zurich

ING IM International is a global asset manager and part of ING Group, a global financial institution of Dutch origin. The successful history of client-focused asset management at ING extends back to 1845 and our roots as a Dutch insurer and commercial bank. In Europe, clients draw upon our more than 40 years' experience in managing pension fund assets in the Netherlands, one of the world's most sophisticated pensions markets.
More information: www.ingim.ch

yourSRI - ESG Data Solutions

yourSRI is a "one stop-solution" for responsible investment products and services providing a wide range of search, comparison, assessment and screening functions. The database offers global coverage for several thousand companies, investment products and research documents as well as a broad variety of reports and surveys.
More information: yourSRI Fact Sheet