What investors need to know about cybersecurity:
How to evaluate investment risks

June 2014

pwc

PwC's Investor Resource Institute

Through the Investor Resource Institute, PwC strives to provide insights to, and receive insights from, the investment community. We offer our views on accounting, auditing, corporate reporting, data security, and a myriad of other issues; as well as transparency about what we do that may be of interest to investors. We host events, both large and small, that are designed to strengthen the bridge not only between PwC and the investment community, but also between investors and others.

IRRCi

The IRRC Institute is a not-for-profit organization established in 2006 and headquartered in New York City. We serve as a funder of environmental, social and corporate governance research, as well as the capital market context that impacts how investors and companies make decisions.

Table of contents

Companies are increasingly vulnerable to incoming cybersecurity threats from new directions and adversaries. Attacks in the form of "hacktivism," corporate espionage, insider and government threats, terrorism, and criminal activity can cost an organization time, resources, and irreparable harm to their reputation if not handled appropriately. Investors can examine corporate disclosures and engage with management to better consider the potential implications of Cybersecurity when assessing investment options. It's more than a technology issue in the back office; it's a critical business issue that can dramatically impact company's competitive position.

Executive summary

The security of information and operational technology has emerged as an enterprise-wide business risk for corporations today. However, these "cyber" risks are not static—they are dynamic, influenced by the growing strategic importance of technology and value of intangible assets created and managed on technology platforms, as well as by an ever-evolving security threat landscape.

As highlighted by recent high profile security breaches, the consequences of poor security include lost revenue, compromised intellectual property, increases in cost, impact to customer retention and can even contribute to C-level executives leaving companies.

Investors are faced with the challenge of measuring and evaluating this risk for their current and potential investments, understanding management's mitigation, and gauging the quality of oversight that the Board of Directors has implemented. Yet the nature of this risk makes it opaque: The sources of cybersecurity threats are hidden and, unfortunately, companies are challenged to accurately assess their exposure to cyber risks themselves even though they have more insights and data than are available to investors. In addition, the current requirements for disclosure of cyber risks are not designed to adequately differentiate between companies' relative readiness, nor are they effective at helping predict which companies are likely to suffer negative impacts due to a security shortcoming.

This paper will outline the trends driving the heightened attention attached to cybersecurity issues and seeks to explore what strategies and approaches investors can pursue in the face of the limited information available. We include a discussion of the potential sources of additional information, beyond a traditional cyber risk disclosure.

This paper does not suggest that investors should steer away from any particular investment due to cybersecurity concerns alone, nor select any security due to comfort at management preparedness. However, the risks and potential business impacts are factors that investors may want to consider when making buy, sale, or engagement and proxy voting decisions. Armed with better information about cybersecurity, investors can play an important role in helping reward companies whose practices are effective at protecting both their customers and their business' information.

Challenges for investors

Disclosures

In 2011 the SEC issued guidance stating that "registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky"[i]. Due to concerns about providing hackers with a roadmap to system vulnerabilities, the SEC clarified that businesses do not need to disclose technical details of these risks. Unfortunately this has resulted in a series of disclosures that rarely provide differentiated or actionable information for investors. A quick read of some example disclosures (provided in the sidebar on the following page) will highlight the challenges facing investors.

Information asymmetry

Moreover, organizations with massive amounts of information on their own security posture still struggle to predict the likelihood and timing related to a cyberattack. Effectively, investors are put in a position of needing to make decisions with limited information, and knowing that even companies with more information still struggle to predict cyber events.

Long-term impacts uncertain

History does not provide a consistent picture on the impact of cybersecurity on a company's performance. Until very recently, most of the long term impact of cyber events was thought to be minimal. Without a doubt there was a direct cost associated with investigating and responding to the breach and often implementing controls around making sure similar events do not happen again. However, in most cases stock prices eventually recovered to pre-breach levels and very limited customer turn over occurred. More recent breaches have seen an impact to customer loyalty and store traffic which has the potential to have a more lasting impact on long term profitability and stock price.

Example 1

"Operational systems and networks have been, and will continue to be, subject to an increasing risk of continually evolving cybersecurity or other technological risks, which could result in the disclosure of confidential client or customer information, damage to <redacted>'s reputation, additional costs to <redacted>, regulatory penalties and financial losses…

<Redacted> has been subject to intentional cyber incidents from external sources, including (i) denial of service attacks, which attempted to interrupt service to clients and customers; (ii) data breaches, which aimed to obtain unauthorized access to customer account data; and (iii) malicious software attacks on client systems, which attempted to allow unauthorized entrance to <redacted>'s systems under the guise of a client and the extraction of client data. For example, in 2012 <redacted> and other U.S. financial institutions experienced distributed denial of service attacks which were intended to disrupt consumer online banking services. While <redacted>'s monitoring and protection services were able to detect and respond to these incidents before they became significant, they still resulted in certain limited losses in some instances as well as increases in expenditures to monitor against the threat of similar future cyber incidents. There can be no assurance that such cyber incidents will not occur again, and they could occur more frequently and on a more significant scale. In addition, because the methods used to cause cyberattacks change frequently or, in some cases, are not recognized until launched, <redacted> may be unable to implement effective preventive measures or proactively address these methods."

Example 2

"A failure in or breach of our operational or security systems or infrastructure, or those of third parties with which we do business, including as a result of cyberattacks, could disrupt our businesses, result in the disclosure or misuse of confidential or proprietary information, damage our reputation, increase our costs and cause losses.

Our businesses are highly dependent on our ability to process, record and monitor, on a continuous basis, a large number of transactions, many of which are highly complex, across numerous and diverse markets in many currencies. The potential for operational risk exposure exists throughout our organization and is not limited to operations functions. Operational risk exposures can impact our results of operations, such as losses resulting from unauthorized trades by employees, and their impact may extend beyond financial losses.

Integral to our performance is the continued efficacy of our internal processes, systems, relationships with third parties and the vast array of employees and key executives in our day-to-day and ongoing operations. With regard to the physical infrastructure and systems that support our operations, we have taken measures to implement backup systems and other safeguards, but our ability to conduct business may be adversely affected by any significant and widespread disruption to our infrastructure or systems. Our financial, accounting, data processing, backup or other operating systems and facilities may fail to operate properly or become disabled or damaged as a result of a number of factors including events that are wholly or partially beyond our control and adversely affect our ability to process these transactions or provide these services. There could be sudden increases in customer transaction volume; electrical or telecommunications outages; natural disasters such as earthquakes, tornadoes and hurricanes; disease pandemics; events arising from local or larger scale political or social matters, including terrorist acts; and cyberattacks. We continuously update these systems to support our operations and growth. This updating entails significant costs and creates risks associated with implementing new systems and integrating them with existing ones."

Example 3

"A breach in the security of <redacted>'s systems could disrupt its businesses, result in the disclosure of confidential information, damage its reputation and create significant financial and legal exposure for the Firm.

Although <redacted> devotes significant resources to maintain and regularly upgrade its systems and processes that are designed to protect the security of the Firm's computer systems, software, networks and other technology assets and the confidentiality, integrity and availability of information belonging to the Firm and its customers, there is no assurance that all of the Firm's security measures will provide absolute security. <Redacted> and other financial services institutions and companies engaged in data processing have reported breaches in the security of their websites or other systems, some of which have involved sophisticated and targeted attacks intended to obtain unauthorized access to confidential information, destroy data, disable or degrade service, or sabotage systems, often through the introduction of computer viruses or malware, cyberattacks and other means. The Firm and several other U.S. financial institutions have also experienced several significant distributed denial-of-service attacks from technically sophisticated and well-resourced third parties which were intended to disrupt consumer online banking services. Despite the Firm's efforts to ensure the integrity of its systems, it is possible that the Firm may not be able to anticipate or to implement effective preventive measures against all security breaches of these types, especially because the techniques used change frequently or are not recognized until launched, and because security attacks can originate from a wide variety of sources, including third parties outside the Firm such as persons who are involved with organized crime or associated with external service providers or who may be linked to terrorist organizations or hostile foreign governments."

Materiality

Looking at past breaches, the tangible costs often land in the $80–200 million range. While this is a significant unplanned cost, this range typically does not fall within the materiality thresholds for most very large companies. Said another way, a cyber-event was often thought to be costly but not deadly to an organization. In addition to more traditional approaches that tend to focus on the costs of breach investigation and reporting, we believe that there are several additional factors that should be considered when determining materiality—including impairment to intellectual property, long term customer satisfaction and customer retention.

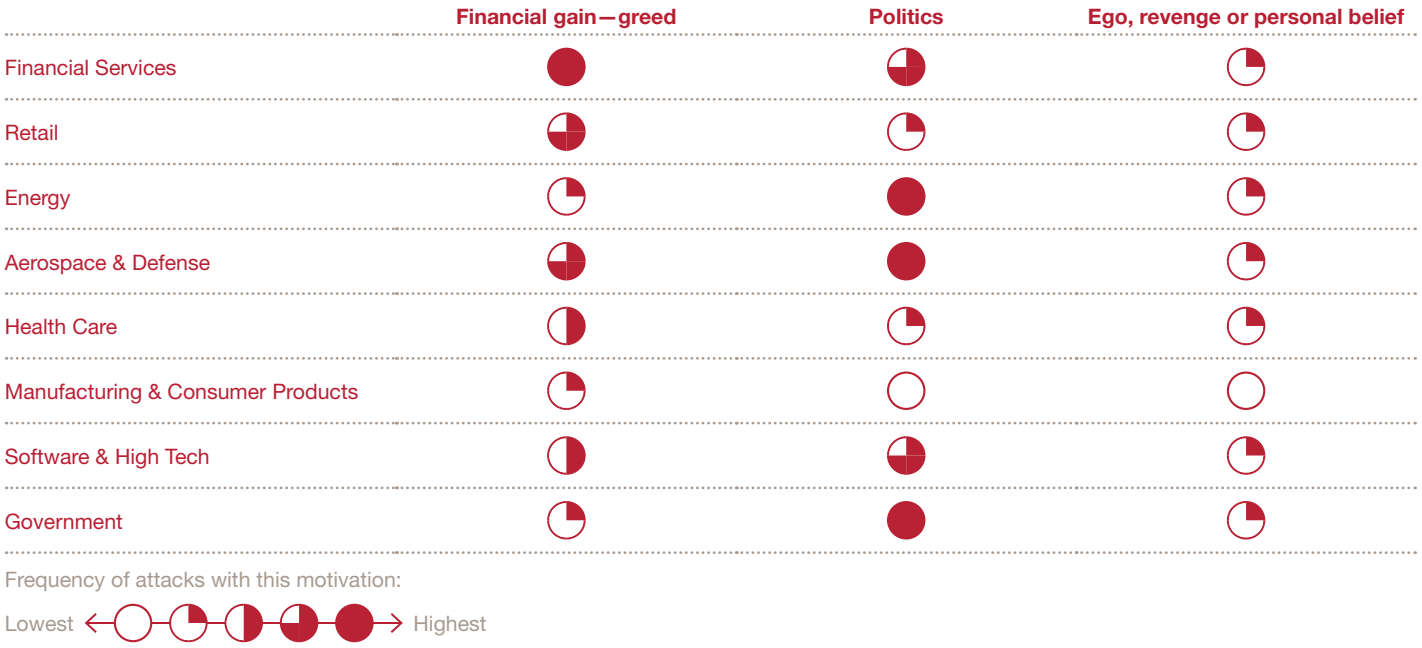
Concentration risk

Another consideration for investors is diversification. Certain industry sectors (e.g., retail, financial services, aerospace & defense) have historically been targeted more heavily than others. Often a specific type of cyberattack (e.g., Distributed Denial of Service attacks[ii], POS Memory Scraping[iii], etc.) will target and impact multiple players within a sector. Although sector diversification has already been considered within most investors' strategies, Cybersecurity risk may not have yet been integrated into this decision-making while a portfolio may span across a number of sectors, if these sectors are all heavily vulnerable to cyberattacks the portfolio may still be subject to concentration risk.

Sector considerations

As noted above, different industry sectors are targeted at varying levels of frequency and based upon different motives. Generally, criminals are motivated by one or more of the following factors: greed, politics, ego, and/or revenge or personal belief. Consequently, these varying motivations may target different industries. The chart below illustrates common impacts and targets by sector, based on our experience.

In addition to these sector-specific considerations, analysis should also focus in on the nature of the firm's products. For instance, does the firm's competitive advantage depend significantly on intellectual property for differentiation? Likewise is the product itself a connected device and part of the "internet of things" and therefore potentially vulnerable to attack directly? These additional factors can create a cyber risk that is often overlooked because it is difficult to quantify and measure.



Understanding the Enterprise Security environment

Cybersecurity has historically been framed in ominous analogies steeped in the notions of attack and contagion. Whether the terms were about viruses, Trojan horses, worms or targeted attacks; the language of cybersecurity tends to focus on the threat actors or attacker side of the equation. However, what an enterprise can do to protect itself from these threat actors is likely of more interest to investors concerned with an organization's cybersecurity posture. Dr. Condoleezza Rice perhaps said it best when speaking more broadly about terrorism, "They have to be right once, we have to be right 100 percent of the time."[1] While this statement was made specifically in reference to terrorism, it does a nice job of summarizing the challenge for business trying to secure cyber space.

Cybersecurity threats are now widespread enough to be a concern universally. The threat actors are numerous enough where there is not a meaningful differentiation between organizations that will or will not experience attacks. However, data shows that breaches can most often be traced to a small number of well-understood, preventable errors on the part of the defenders. It seems today the question is not will a firm be breached but can it limit the information that is exposed and how does the firm respond. Consequently, an investor's differentiation between companies could lie not only in understanding their ability to defend against those attacks by avoiding common errors but also in the companies' preparedness to respond quickly to contain or mitigate the potential harm.

Translating concern into effective security

It has long since ceased being a challenge within organizations to obtain senior management attention or commitment to the notion of security. The 2014 PwC Global State of Information Security Survey (GSISS) results shows some variability in how that commitment translates into budget, resources, and seniority of security staff. However, while resourcing is a definite concern, the most recent set of breaches provides an important lesson that resources alone do not immunize a company from harm. Indications in one breached company's own disclosures indicate that management both contemplated and understood the risk and the impact that a cybersecurity breach would pose to their business. In addition, media

1 *National Commission on Terrorist Attacks upon the United States*, Ninth Public Hearing, Thursday, April 8, 2004

reports indicate that the security professionals within this company were investing significant funds in security technology. Yet the impact of the money and the management attention was not enough to prevent a massive breach.

It is important to note that these types of preventable errors lie predominantly within the realm of companies' IT operations. Humans can fall prey to phishing[iv] attacks, be duped into visiting malicious websites, or lose media containing sensitive data; but all these instances need weak passwords, poor network segmentation, lack of monitoring, and other IT flaws to become a significant breach. In the following section we will explore other indicators of IT's effectiveness around security.

What does effective security look like?

There is no shortage of guidance available on how to develop an effective cybersecurity program. The challenge for investors is simplifying this guidance to a few key items that can be identified and understood by those outside the company. One thing is for sure—simply being compliant with current laws and regulations does not mean a company is secure. For instance, the retail companies that experienced breaches in late 2013 and early 2014 all appeared to be PCI compliant[v] prior to these breaches occurring. But one challenge with requiring specific technical controls is that hackers continue to innovate and improve their techniques. So controls focused on preventing the last attack may not adequately address the next one. The recently released NIST Cybersecurity Framework, which was drafted by the Commerce Department's National Institute of Standards and Technology (NIST), leverages and integrates industry leading cybersecurity practices that have been developed by organizations like NIST, Federal Financial Institutions Examination Council (FFIEC), and the International Standardization Organization (ISO)[vi]. The Framework provides an iterative process designed to evolve in synch with changes in cybersecurity threats, processes, and technologies and provides some high-level considerations for investors. It is organized by five continuous functions:

- **Identify:** An understanding of how to manage cybersecurity risks to systems, assets, data, and capabilities.
- **Protect:** The controls and safeguards necessary to protect assets or deter cybersecurity threats.
- **Detect:** Continuous monitoring to provide proactive and real-time alerts of cybersecurity-related events.
- **Respond:** The policies and activities necessary for prompt responses to cybersecurity incidents.
- **Recover:** Business continuity plans to maintain resilience and recover capabilities after a cyber-breach.

It's unlikely that investors will be given access to results of gap assessments against frameworks such as NIST or ISO. In fact, this would likely do more harm than good as it would provide a blueprint of the company's potential weaknesses. However, investors can engage with company management about these issues, potentially posing the following questions:

- Does the organization have a Security & Privacy executive that reports to a senior level position within the company? What are the skills, experiences and qualifications of this executive?
- Does the organization have a documented cybersecurity strategy that is regularly reviewed and updated? How is the board engaged in the cybersecurity strategy and review process?
- Does the organization perform periodic risk assessments and technical audits of its security posture?
- Can senior business executives explain the challenges of cybersecurity and how their company is responding? Does the "tone at the top" seem to make security a priority?
- What is the organization doing to address security with its business partners?
- Has the company addressed its sector-based vulnerability to cyberattack (see chart on page 7)?
- Does the organization have a response plan for a cyber incident? Is it tested regularly through simulations and table top exercises? Does it include testing with key 3rd party relationships?

Conclusion

It is difficult for any person outside the company to quantify the potential exposure of cyberattacks for a specific organization. But investors can understand which industry sectors are more at risk than others, and can identify the types of companies that are likely to possess more personal or financial information than others. Likewise, investors can focus on the specific industry leading practices outlined within this paper to determine if the company is reasonably prepared for a cyberattack. In today's interconnected world, it is not a question of whether a company will have a cyber security incident; rather it's a matter of when and how prepared the company is to respond and minimize the impact of the incident.

- Cybersecurity risk is dynamic. Risks continue to evolve and accelerate and firms must constantly improve and react.
- Cybersecurity concerns are important considerations when diversifying portfolio risk.
- Disclosures can help investors understand management's ability to detect and respond to cybersecurity threats.
- But shareholder-corporate engagement around cybersecurity can provide even greater insights for investors.
- Investors can use the questions provided in this document as the core of that engagement.

Endnotes:

i. See Securities and Exchange Commission, Division of Corporate Finance, CF Disclosure Guidance: Topic No. 2, Cybersecurity; October 13, 2011; at www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. Also see Item 503(c) of Regulation S-K; and Form 20-F, Item 3.D.

ii. A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users.

iii. POS Memory Scrapers are malicious programs that search point-of-sale (POS) systems for bank card information stored briefly in POS devices. Typically, the malware captures the data stored on the bank card's magnetic stripe in the instant after it has been swiped at a POS terminal, which information can then be used to create closed copies of the bank cards.

iv. Phishing is the attempt to acquire sensitive information such as usernames, passwords, and bank card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

v. The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that companies that process, store or transmit credit card information maintain a secure environment.

vi. See National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014; at www.nist.gov/cyberframework/.

www.pwc.com

For further information, please contact:

Kayla J. Gillan
Leader, PwC Investor Resource Institute
Office: 202 312 7525
Mobile: 646 476 1380
kayla.j.gillan@us.pwc.com

Joseph Nocera
Principal, PwC
Office: 312 298 2745
joseph.nocera@us.pwc.com

Peter Harries
Principal, PwC
Office: 213 356 6760
Mobile: 602 750 3404
peter.harries@us.pwc.com