Ian de Verteuil
1 (416) 594-7462
Ian.deVerteuil@cibc.com

Shaz Merwat
1 (416) 956-6428
shaz.merwat@cibc.com

Portfolio Strategy

INDUSTRY UPDATE

August 20, 2017

The Known Unknown

A Beginner's Guide To Understanding Cyber-risk In Investment Portfolios

What's The Event?

The risks around cyber-security and the importance of protecting proprietary data are well known across society – whether it be governments, corporations or even individuals. Within corporations, the risk is often cited by management and the board of directors. According to studies, however, companies still struggle with mitigating the risk of a cyber-breach.

From our perspective, it is likely we will have a major cyber-crime issue at one or more large public Canadian companies over the next year or two. In our opinion, Service companies are most at risk, including Financial Services. As such, forewarned is forearmed.

Implications

Should investors care? On the one hand, there were few signs that even major breaches have had significant impact on stock prices. For perspective, a study released by CGI suggested that companies experiencing "Severe or Catastrophic" cyber-attacks saw their share prices decline by about 2%. For equity investors, such a stock price decline would certainly not fit into the "Severe or Catastrophic" category!

On the other hand, it is hard to believe companies that allow detailed personal data of their customers to be exposed are only marginally affected. Surely beyond any short-term costs from various fines, remediation or ransomware, there could be long-term negative impacts to brand value. It is also possible that analysis of stock price impact goes well beyond a single security - affecting sentiment across the overall sector.

This report attempts to do three things – all of which should be useful to generalist portfolio managers. First, we provide an overview of the current cyber-crime environment. Second, we review a handful of recent attacks so as to see how these events occur, and what are their implications. Third, we provide a list of questions that PMs can ask senior executives, so as to gauge corporate readiness.

Though we focus on risks arising from breaches, we highlight additional upcoming reports from Stephanie Price on the cyber-security opportunity.

All figures in Canadian dollars, unless otherwise stated.

For required regulatory disclosures please refer to "Important Disclosures" beginning on page 11.

Cyber-crime 101

From our perspective, investors have focused more on the opportunities from cyber-crime, i.e. investing in companies that offer services to defend against such an attack, rather than the risk of a corporation being hacked. One reason may be that investors don't currently understand the rudimentary issues or the extent of cyber-crime.

Cyber-crime experts will tell you that any company or individual that uses a computer or mobile device is vulnerable, and most are under attack as this document is being read. Several factors are at play.

The risks often arise from within.

First, the technology users themselves (employees and management) have limited understanding of the risks they are facing. Though processes and systems encourage caution, the reality is still human "error", or more appropriately human naiveté, is most often the cause of the vulnerability. To be fair though, the pace of change needed to properly defend against cyber-crime is changing so fast that humans would always have a difficult time keeping up.

Second, the end-consumer is driving rapid growth of on-line connectedness which, in and of itself, exposes organizations. A company may have difficulty identifying whether the connected individual is a customer, or a criminal. Every smart phone, tablet, watch, printer and most pieces of equipment provide a breeding ground for cyber-attacks.

Third, the incentives to cyber-criminals are attractive. Few are ever caught and the pay-offs can be substantial. The stories of "help desks" used to assist in paying ransomware are true. Fourth, the reality is cyber-crime is occasionally state-supported resulting in well-financed, concerted efforts.

The computer or software on your desk has certainly arrived with vulnerabilities.

Lastly, computers themselves are vulnerable. Today, they are largely made through an integrated supply chain with chips, circuit boards and operating systems all sourced separately. It is difficult to be confident that the machine (or device) didn't arrive with known vulnerabilities already built in.

Not surprising, the industry has its own terminology. In Exhibit 1 below, we provide a handful of terms for the cyber-rubes who remember the old days when there was limited downside to fishing!

Exhibit 1. Basic Terminology In Cyber-crime

Breach Type	Breach Description
Malware	A variety of common forms of software that run on a computer with malicious intent (viruses, trojans, worms, etc.). Malware can be used to destroy, alter or steal data or alter hardware behavior.
Zero Day	A 'zero-day' attack exploits previously unknown vulnerabilities in applications/OS, making it difficult for security systems (e.g., anti-virus, intrusion alerts) to detect and stop it.
Phishing	Typically, an email, often sent to thousands of users designed to reveal sensitive information or install malware. Spear phishing emails are carefully crafted messages, leading users to believe they are legitimiate, including Business Email Compromise attacks (BEC), also known as "CEO fraud", wherein cyber criminals are able to impersonate company executives (primarily CEOs) by successfully phishing their inbox.
Cracking	When an attacker tries to gain access to a computer system by guessing passwords. Involves using automation tools or social engineering to narrow the list of potential passwords.
Ransomware	A form of malware that prevents a user accessing their files by encrypting them and then demanding a ransom payment to unlock the files. In many instances the victims are repeat victims, and also sometimes can pay but the files are never unlocked.
Spoofing	When an attacker or malicious program successfully acts on another person's or program's behalf by impersonating data. This is usually done on a network and tends to involve re-routing or replicating an IP, DNS (Domain Name System) or ARP (Address Resolution Protocol).
Denial of service	Attacker disrupts a user's network access by overloading it with connection requests. A distributed denial of service attack (DDoS) uses hundreds or thousands of computers around the world, known as a botnet, to mount this attack, making it difficult to block.
Botnet	A user's computer may be infected with a type of malware that uses the computer to distribute malware, mount a DDoS attack, or other illicit function, all without the user's knowledge.

Source: CGI UK and CIBC World Markets Inc.

It is difficult to say whether the "good guys" or "bad guys" are winning the cyber-crime battle. According to Symantec, on some metrics the situation is improving, while on others things are deteriorating. As we show in Exhibit 2, there is no clear pattern, though the breaches do seem to be getting bigger, if not more frequent. Note that Symantec only includes the breaches in the year it occurred, not the year it was reported, so Yahoo!'s disclosure in 2016 of its 2013 breach of 1 billion user accounts is not in Exhibit 2.

Exhibit 2. Data Breaches And Malware Instances, 2014-2016

Year	Breaches	Number of Identities Stolen	Identities per Breach	Mega-breaches	Overall E-mail Malware Rate
2014	1,523	1,226,138,929	805,081	11	1 in 244 (0.41%)
2015	1,211	563,807,647	465,572	13	1 in 220 (0.45%)
2016	1,209	1,120,172,821	926,528	15	1 in 131 (0.76%)

Note: 1) A Mega-breach is defined as a breach with over 1 million identities exposed; 2) E-mail malware rate refers to frequency of emails containing malware per total emails sent. Source: Symantec and CIBC World Markets Inc.

Not surprisingly, the U.S. has been the most targeted country. Depending on the metric and breach type, it represents from one-third to two-thirds of all attacks. Canada ranks quite high, i.e. poorly, materially higher than its share of global GDP. One possible explanation is the interconnectivity with U.S. corporations.

From an investor perspective, it is also worth understanding the sectors most targeted. As shown in Exhibit 3, Services companies appear much more at risk than Manufacturing companies as two-thirds of all breaches are in Services-oriented companies (including Financial Services). Within "Services", the two biggest are Business Services and Health Care. If we itemized these separately (not shown in Exhibit 3), these sub-sectors would be 248 breaches and 115 breaches, respectively, making them the biggest and fourth biggest segments.

Exhibit 3. Sector Breakdown Of Attacks

Rank	Industry	Number of Breaches	Percent of Total
1	Services	452	44.2%
2	Financial Services	226	22.1%
3	Manufacturing	116	11.4%
4	Retail Trade	84	8.2%
5	Transport & Public Utilities	75	7.3%
6	Wholesale Trade	32	3.1%
7	Construction	20	2.0%
8	Mining	8	0.8%
9	Public Administration	6	0.6%
10	Nonclassifiable Establishments	3	0.3%
	All Industries	**1,022**	**100%**

Source: Symantec and CIBC World Markets Inc.

In the U.S., mandatory breach notification has been a reality in most states for several years. Even so, in the cases of Yahoo! and JP Morgan, it does appear that government involvement has played a role in investigating and identifying the attacks. In Europe, it will become compulsory from May 2018 as the General Data Protection Regulation (GDPR) comes into full force.

Compliance with GDPR is not simply a tick-box exercise for lawyers: it requires a detailed understanding of what each particular business does, what personal data it collects and for what purposes, who it is sent to, where it resides geographically and how it is protected. Knowing this information will be a key starting point for any effective compliance program.

Our impression is that Canada has lagged other jurisdictions in government-corporate interaction and in mandating disclosure. The good news is that a non-profit organization with extensive Canadian bank involvement has been developed – the entity is called the Canadian Cyber Threat Exchange (CCTX). One thrust is a coordinated effort to create linkages into the Department of Public Safety and Canada's electronic spy agency, the Communications Security Establishment (CSE).

Share Price Impact Is Limited – So Far

It is difficult to believe that compromising company's consumer data on a massive scale would not have a material impact on share price, but that is what evidence suggests. We show five tangible case studies in this section of the report (over the past five years) that were large, and involved public entities. The impact on value of the targeted entity ranged from negligible to 7% (say 2.4% on average).

While we would not claim that our analysis is terribly robust given the limited data set, it is interesting that this broadly aligns with a CGI U.K. study with Oxford Economics which attempted to quantify the impact of a data breach on share price performance. The authors concluded that on average, companies that reported major or catastrophic breaches (as defined by CGI) underperformed their peers by about 1.8%.

Having said that, the CGI report does suggest the impact is getting larger over time. Furthermore, we believe that the ramifications for some companies will be more material. Specifically, we would note that companies that are engaged in

M&A might have a bigger impact (example Yahoo!). We would also expect regulated companies that are hacked may have bigger issues as oversight or penalties could be applied.

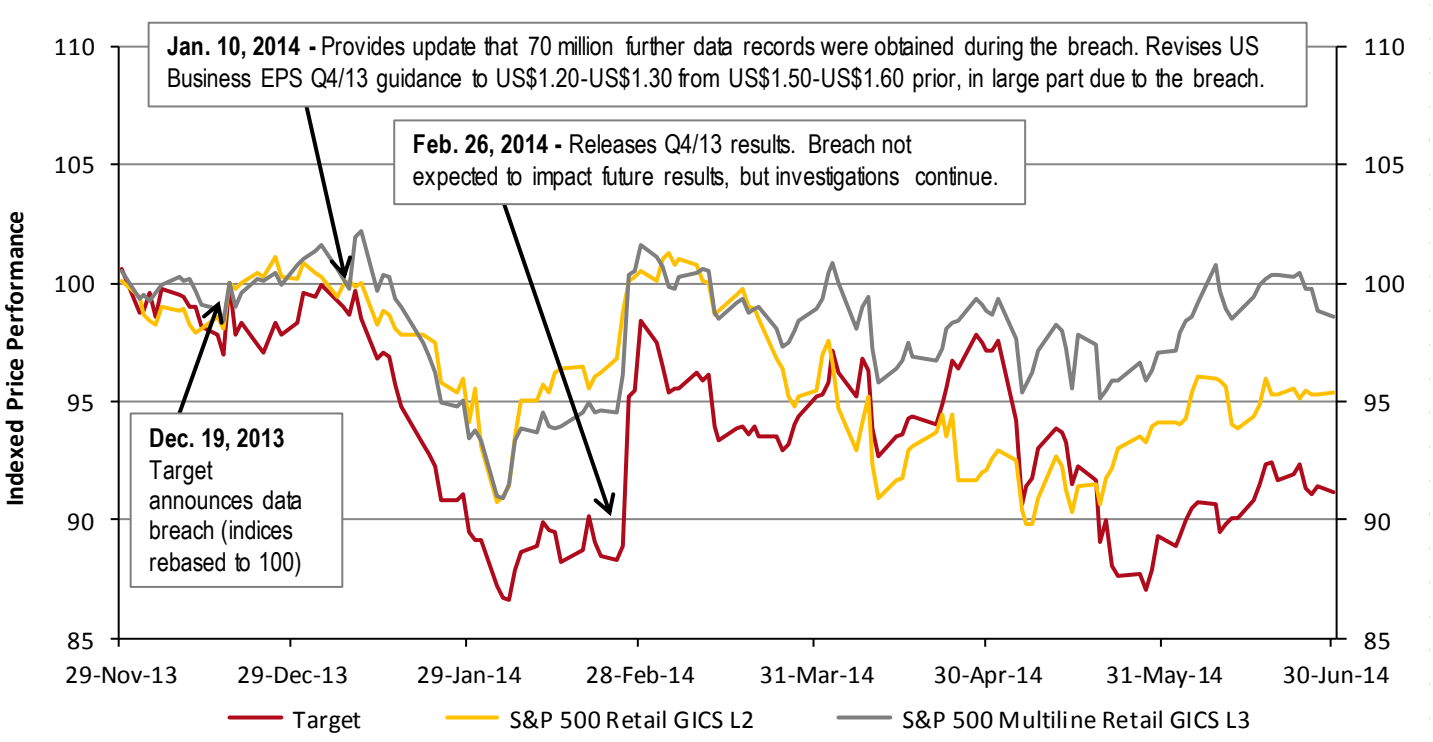
We would also note that the benchmark that we use to compare the severity of the stock price impact could also be affected, i.e. a breach of a major bank could affect the bank "index" as well. Our point here is that simply using the ~2% impact number probably understates the full impact. Below, we provide a brief review of a handful of significant breaches.

1. Target 2013/2014 (~5%)

In late 2013, Target was the target (no pun intended) of a major data breach, in which over 110 million records (40 million in customer credit/debit card information) were obtained. The company was informed by the Dept. of Justice in mid-December 2013, and on December 19 publicly verified the data breach.

The timing could not have been worse, at the eve of Christmas, and note there was about ~2% of relative underperformance in the equity relative to peers (as seen in Exhibit 4 below). The company did a good job of keeping customers informed throughout the process (seven press releases were issued from Dec. 17 to Dec. 27), but generally, the company didn't seem to exhibit any additional price impact through the Holidays.

Exhibit 4. Effect On Target's Share Price Performance From Reported Data Breach



Source: Bloomberg, company reports and CIBC World Markets Inc.

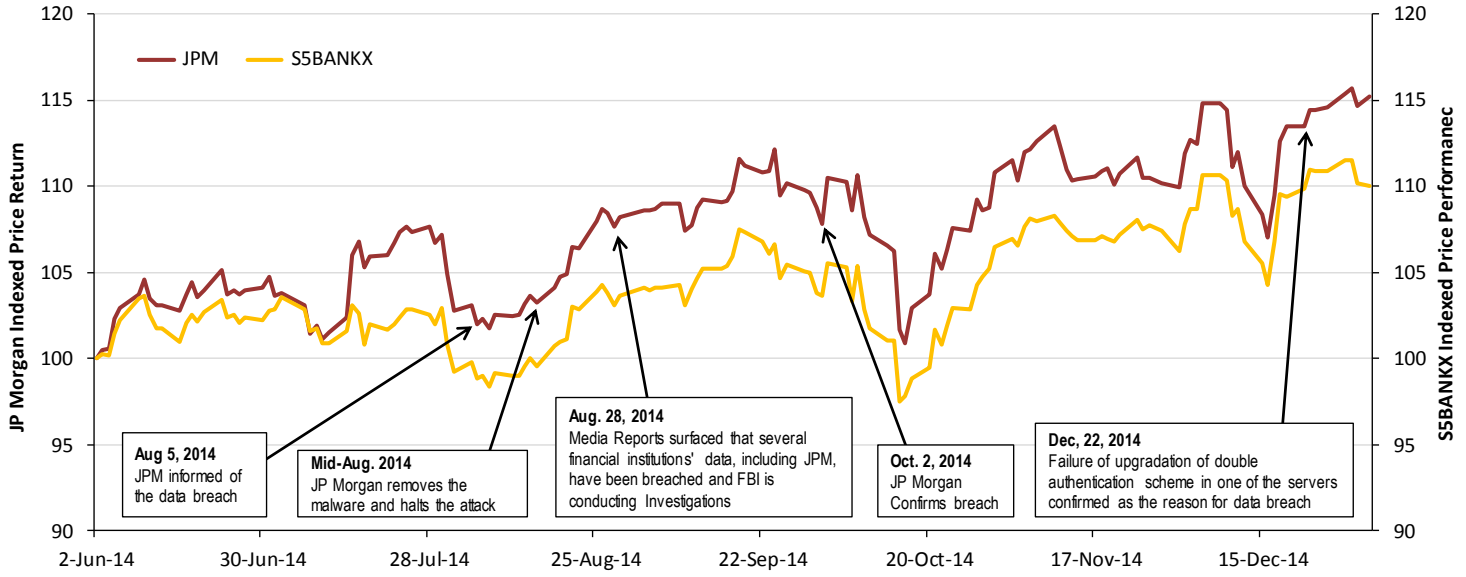
When the company did, however, quantify the impact of the breach and revise guidance, the impact on the share price was more meaningful, sliding to about 400 basis points of underperformance by the end of January. The stock rallied with Q4/13 results, but overall the large movements in the stock only really came once the impact of the breach was quantified to investors on an EPS basis.

Similar to the JP Morgan breach (detailed later), the impact on Target's reputation went beyond valuation, as the CEO lost his job within six months. Target also implemented a new Chief Information Officer and accelerated the adoption of chip-enabled technology (encryption) across its portfolio.

2. JP Morgan Chase 2014 (No Obvious Stock Price Impact)

One would have expected that a breach at one of the largest banks in America, involving 76 million households and 7 million small businesses, would be extremely damaging. For whatever reason, the event did not seem to cause many problems with JP Morgan's shares. As we show in Exhibit 5, there are few if any obvious signs that unsettled investors – at least vis-a-vis peers.

Exhibit 5. Effect On JP Morgan's Share Price Performance From Reported Data Breach



Source: Bloomberg, company reports and CIBC World Markets Inc.

Now, there were extenuating circumstances. First, JP management were clear that although contact details were stolen, sensitive information (account numbers, passwords and Social Security numbers) was not accessed. Second, there had been news articles from months earlier suggesting data breach attempts on several US financial institutions, so one could argue that the market had been sensitized to this possibility.

In the aftermath, implications for JP Morgan appeared to be modest – even beyond the short-term impact. The company announced a US$250 million bump in spending on cyber-security. The only additional apparent backlash came from the "reassignment" of JP's Chief Information Officer.

3. Yahoo! 2016 (~7%)

In September 2016, Yahoo! reported the company's network suffered a major data breach in late 2014. Yahoo! revealed the data compromised pertained to email addresses, telephone numbers, birth dates, hashed passwords and in some cases, security questions and answers. Initially, the announcement suggested that the hack was in late 2014, and related to 500 accounts. Three months later, Yahoo! discovered that it had also been hacked in 2013 – and that 1 billion user accounts were stolen.

Yahoo! undertook a number of steps to protect its clients including the following: invalidated all previous cookies, recommended users use a Yahoo!-specific authentication tool, invalidated all unencrypted security questions and recommended a variety of now well-accepted customer behaviors (being cautious on phishing, changing passwords, checking accounts for suspicious activity, etc.). In March 2017, the U.S. Department of Justice charged Russian spies and hackers with the data breaches.

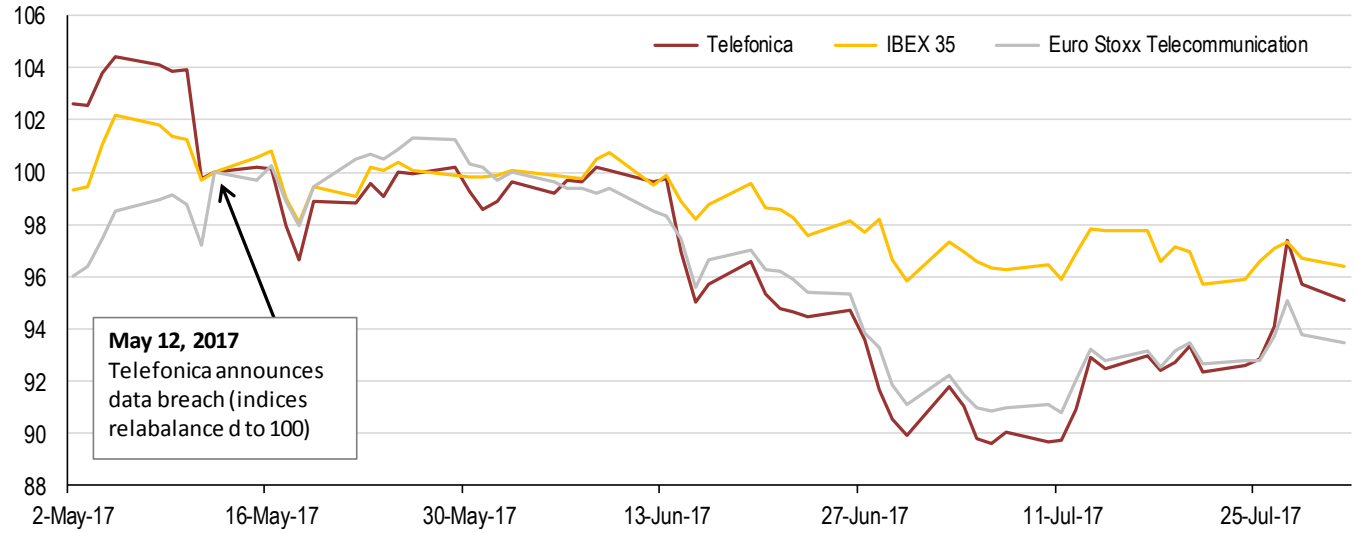
One unique (and quite useful) aspect of this situation arises because Yahoo! and Verizon were in the midst of a transaction. This provides relatively clear indication of the impact on value. Specifically, the acquisition price was adjusted lower by US$350 million – representing a 7% drop in value.

4. Telefonica 2017 (No Obvious Stock Price Impact)

Very recently, Telefonica was hit by a large-scale ransomware attack (effectively WannaCry Version 2.0) that eventually led to employees cutting their internet connections or turning off their computers, as the company was largely unprepared for the attack. The extent of the attack was wide-spread, affecting up to 85% of employee computers, but telecommunication services remained intact throughout. The financial loss was largely expected to reside in lost work hours, more than anything else.

Overall, the data breach seems to have had a negligible impact on share price performance. What makes the Telefonica case somewhat different relative to the others was the lack of updates (or any mention really) of the effect of the data breach. The company put out an initial press release verifying the attack, but didn't even mention the attack in its Q2/17 press release one month later, nor has it done so to date. This is starkly different than how Target approached the matter, but to be fair, the Telefonica incident may have been less severe, as certainly indicated in its two-sentence press release. Nonetheless, the incident did not seem to have an impact on its share price performance relative to peers.

Exhibit 6. Effect On Telefonica's Share Price Performance From Reported Data Breach

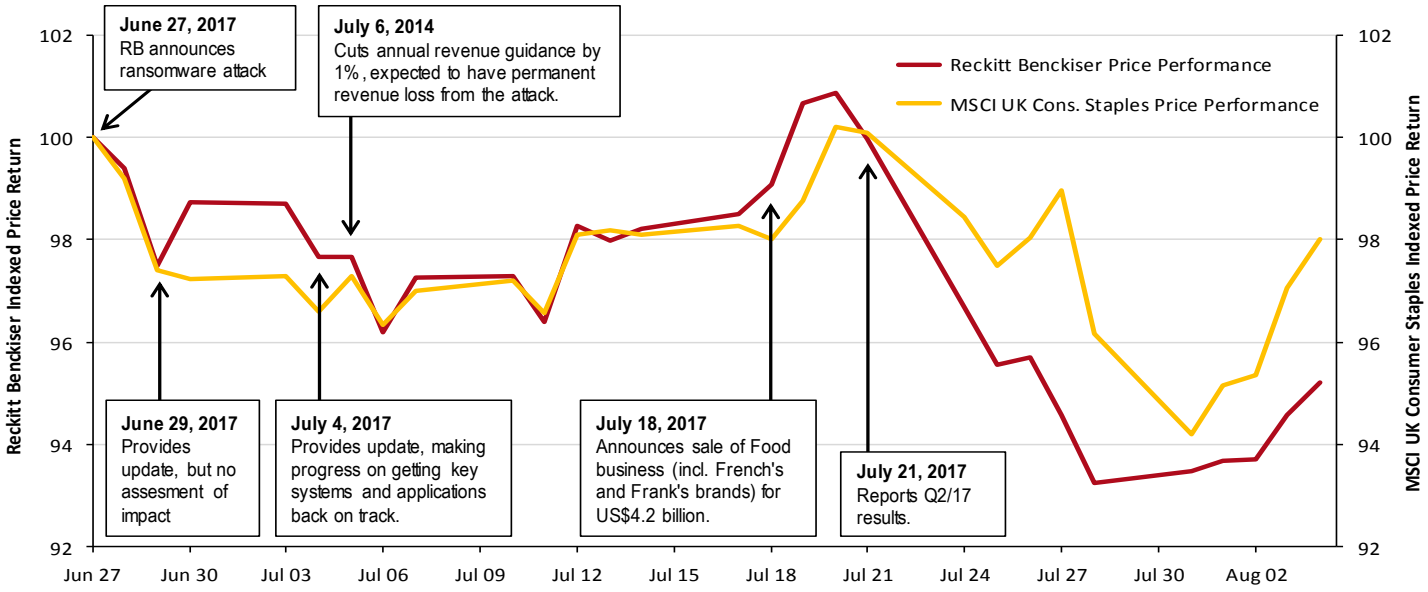


Source: Bloomberg, company reports and CIBC World Markets Inc.

5. Reckitt Benckiser (No Obvious Stock Price Impact)

Reckitt Benckiser was the most recent to experience a cyber-attack, falling victim to the Petya ransomware virus, believed to have originated out of Ukraine. The stock performed relatively in line with its peers during the early stages – in fact, there seemed to never really be any point of material underperformance resulting from the attack.

Exhibit 7. Effect On Reckitt Benckiser Share Price From Ransomware Attack



Source: Bloomberg, company reports and CIBC World Markets Inc.

One contributing factor could have been that this was a very widely reported attack that affected numerous parties, including global shipping giant Maersk and national airports within Ukraine. Over 10 countries were hit, and the level of sophistication from the attack could have diluted the effect to any one company being seen as uniquely inadequate in their IT security.

As a result of the attack, the company revised annual 2017 revenue guidance downwards to 2% (from 3%), and stated that due to certain data being un-encrypted (i.e., now lost forever), the company was expecting a certain level of permanent revenue loss.

There are two characteristics of the Reckitt Benckiser attack that are particularly interesting: 1) cyber-experts believe the purpose of the Petya attack was not for monetary gain, but rather purely for destruction; and 2) the company closed a US$4.2 billion sale of its Foods business within a month of the attack. In contrast, previous ransomware attacks have primarily dealt with gaining an economic benefit. On the M&A front, perhaps because the sale was just a division of the business and not the entire company itself (where a corporate IT function is most likely to reside), the effects of the breach were not as significant, relative to the Verizon-Yahoo! deal for instance.

A Few Questions To Ask

So if the impact of cyber-crime has been minimal so far, is this something that Portfolio Managers can ignore? In our opinion, the answer is no. Whatever the evidence to date, we believe that the frequency and severity of cyber-attacks will increase over time. The culprits are seldom caught, users are frequently too lax in their own processes and the vulnerability increases as more devices and connected machines are employed.

In our opinion, shrewd investors will need a series of questions that provide insight into how seriously the c-suite of a company takes cyber-risk. Below are a list of suggested questions and possible answers. The list below is quite exhaustive with different questions being appropriate for each of the CEO, the CIO or the Head of Investor Relations.

In our opinion, Services companies are most vulnerable sector – including Financial Services. While there is little doubt that these companies take the threat extremely seriously, the data is quite clear – they are the most frequent and attractive target for cyber-criminals.

- **Who is responsible for cyber-security?** The CEO should be responsible for driving security governance, investment and planning, but day-to-day responsibilities are often delegated. Each employee has a part to play.
- **Do you have a current cyber-incident response plan? Can we see it?** The plan should detail who is responsible in managing a breach, who else is involved in the process (Communications, Legal, IT specialists, etc.) and how current is the plan.
- **Can someone in the organization brief me on your cyber-risk profile?** In essence, it matters more whether the company can articulate responsibility, which should provide information as to how rigorously they've thought of their cyber-security management.
- **How many attacks were seen last quarter/month/week?** The key to a good response here is simply having awareness to the current status.
- **What have you learned from previous cyber incidents?** Incidents should be treated as opportunities to learn and bridge the gap. Zero reported threats could easily mean breaches are yet to be identified.
- **Have any independent tests been done?** With increasing regulation, it will be paramount for companies to demonstrate their fiduciary duty towards stakeholders with a responsible risk mitigation process in place. Third-party verification would limit any possible legal/regulatory ramifications from a future breach.
- **Is cyber-security classified as one of your corporate risks?** IT risks can often be arcane to the average employee, but the translation of the technical nature of the risk needs to transcend to the senior management and the board of directors.
- **How much would it cost if you lost all your IT systems for a day?** This is meant to gauge whether Sr. Management has a true understanding of the cost of an IT interruption to operations, which often are underestimated.
- **What is the most valued information at this firm?** Ideally, the company has a more robust data protection system in place around the company's 'crown jewels.' It also gives management the practice of knowing where the most impactful breaches are most likely to occur.

- **What is the current annual cyber-security budget?** Typically, this amounts to about 5% of an IT budget, although more recently that number has increased to around 10%.

- **How is cyber-security risk disclosed in company disclosure?** This should allow investment professionals to be able to keep up to date with how management is adapting to the nature of cyber-security.

- **Is there business interruption insurance in place to deal with a cyber-breach?** Understanding whether the company is covered in case of a cyber-breach will help investors evaluate the potential fallout from a possible incident.

- **Do you have communication obligations to clients, employees, investors, regulators, etc. in case of a cyber-breach? Is there legal advice to guide you?** Understanding roles and responsibilities should allow for clear and concise messaging to customers, the investment community and regulators in case of an incident. This should help reduce volatility and speculation on share price should an event ever occur.

- **Do you have a back-up site in place? Would the transfer be seamless?** Effectively, what is Plan B?

- **Are employees well-versed as to how to deal with a cyber-attack?** This question should help provide color as to how well the risk is understood across the organization. If an employee's system is overtaken by malware, does he/she know what to do?

- **Is there a call-tree/contact list in place?** Should be easily accessible so as not to waste time in bureaucracy in case of an actual cyber event.

- **Has the firm undertaken fire drills to test the response plan?** Practice makes perfect, and routine mock exercises should be run to test operational procedures.

- **Does the company participate in industry forums?** Hacktivists are extremely sophisticated and sometimes even state-sponsored. Shared learning and best practices are a way to stay ahead of the curve.

- **What are the top 5 cyber-risks you face today?** The ability to specifically pinpoint risks should provide reassurance that the company has spent the time to think this through. It also can gauge how the company sees the risks evolving over time.

We understand that investment professionals (like us) also struggle to truly comprehend the full extent and implications of a cyber-breach. However, we believe asking a handful of these questions would provide investors insight as to how seriously this risk is taken at certain companies.

We note that the list of questions and insights above were partially established by CIBC, and should also be credited to discussions arising from our June cyber-security session with executives from CGI, the Global Risk Institute and eSentire. Many thanks to all.

As well, we highlight that while this report focuses on portfolio risks, there will be upcoming reports from our colleague Stephanie Price on cyber-crime opportunities.

IMPORTANT DISCLOSURES:

Analyst Certification: Each CIBC World Markets Corp./Inc. research analyst named on the front page of this research report, or at the beginning of any subsection hereof, hereby certifies that (i) the recommendations and opinions expressed herein accurately reflect such research analyst's personal views about the company and securities that are the subject of this report and all other companies and securities mentioned in this report that are covered by such research analyst and (ii) no part of the research analyst's compensation was, is, or will be, directly or indirectly, related to the specific recommendations or views expressed by such research analyst in this report.

Analysts employed outside the U.S. are not registered as research analysts with FINRA. These analysts may not be associated persons of CIBC World Markets Corp. and therefore may not be subject to FINRA Rule 2241 restrictions on communications with a subject company, public appearances and trading securities held by a research analyst account.

Potential Conflicts of Interest: Equity research analysts employed by CIBC World Markets Corp./Inc. are compensated from revenues generated by various CIBC World Markets Corp./Inc. businesses, including the CIBC World Markets Investment Banking Department. Research analysts do not receive compensation based upon revenues from specific investment banking transactions. CIBC World Markets Corp./Inc. generally prohibits any research analyst and any member of his or her household from executing trades in the securities of a company that such research analyst covers. Additionally, CIBC World Markets Corp./Inc. generally prohibits any research analyst from serving as an officer, director or advisory board member of a company that such analyst covers.

In addition to 1% ownership positions in covered companies that are required to be specifically disclosed in this report, CIBC World Markets Corp./Inc. may have a long position of less than 1% or a short position or deal as principal in the securities discussed herein, related securities or in options, futures or other derivative instruments based thereon.

Recipients of this report are advised that any or all of the foregoing arrangements, as well as more specific disclosures set forth below, may at times give rise to potential conflicts of interest.

CIBC World Markets Corp./Inc. Stock Rating System

Abbreviation	Rating	Description
Stock Ratings		
OP	Outperformer	Stock is expected to outperform similar stocks in the coverage universe during the next 12-18 months.
NT	Neutral	Stock is expected to perform in line with similar stocks in the coverage universe during the next 12-18 months.
UN	Underperformer	Stock is expected to underperform similar stocks in the coverage universe during the next 12-18 months.
NR	Not Rated	CIBC World Markets does not maintain an investment recommendation on the stock.
R	Restricted	CIBC World Markets is restricted (due to potential conflict of interest) from rating the stock.
Stock Ratings Prior To December 09, 2016		
SO	Sector Outperformer	Stock is expected to outperform the sector during the next 12-18 months.
SP	Sector Performer	Stock is expected to perform in line with the sector during the next 12-18 months.
SU	Sector Underperformer	Stock is expected to underperform the sector during the next 12-18 months.
NR	Not Rated	CIBC World Markets does not maintain an investment recommendation on the stock.
R	Restricted	CIBC World Markets is restricted (due to potential conflict of interest) from rating the stock.
Sector Ratings (note: Broader market averages refer to S&P 500 in the U.S. and S&P/TSX Composite in Canada.)		
O	Overweight	Sector is expected to outperform the broader market averages.
M	Marketweight	Sector is expected to equal the performance of the broader market averages.
U	Underweight	Sector is expected to underperform the broader market averages.
NA	None	Sector rating is not applicable.

"Speculative" indicates that an investment in this security involves a high amount of risk due to volatility and/or liquidity issues.

Ratings Distribution*: CIBC World Markets Corp./Inc. Coverage Universe

(as of 20 Aug 2017)	Count	Percent	Inv. Banking Relationships	Count	Percent
Outperformer (Buy)	142	47.8%	Outperformer (Buy)	142	100.0%
Neutral (Hold/Neutral)	131	44.1%	Neutral (Hold/Neutral)	131	100.0%
Underperformer (Sell)	16	5.4%	Underperformer (Sell)	16	100.0%
Restricted	8	2.7%	Restricted	8	100.0%

Ratings Distribution: Portfolio Strategy Coverage Universe

(as of 20 Aug 2017)	Count	Percent	Inv. Banking Relationships	Count	Percent
Outperformer (Buy)	0	0.0%	Outperformer (Buy)	0	0.0%
Neutral (Hold/Neutral)	0	0.0%	Neutral (Hold/Neutral)	0	0.0%
Underperformer (Sell)	0	0.0%	Underperformer (Sell)	0	0.0%
Restricted	0	0.0%	Restricted	0	0.0%

*Although the investment recommendations within the three-tiered,relative stock rating system utilized by CIBC World Markets Corp./Inc.do not correlate to buy, hold and sell recommendations, for the purposes of complying with FINRA rules, CIBC World Markets Corp./Inc. has assigned buy ratings to securities rated Outperformer, hold ratings to securities rated Neutral, and sell ratings to securities rated Underperformer. The distributions above reflect the combined historical ratings of CIBC World Markets Corp. and CIBC World Markets Inc.

Important disclosures required by applicable rules can be obtained by visiting CIBC World Markets on the web at http://researchcentral.cibcwm.com/. Important disclosures for each issuer can be found using the "Coverage" tab on the top left of the Research Central home page. Access to the system for rating investment opportunities and our dissemination policy can be found at the bottom of each page on the Research Central website. These important disclosures can also be obtained by writing to CIBC World Markets Corp., 425 Lexington Avenue, New York, NY 10017 (212-856-4000) or CIBC World Markets Inc.,161 Bay Street, 4th Floor, Toronto, ON M5H 2S8, Attention: Research Disclosures Request.

CIBC World Markets Corp./Inc. Price Chart

For price and performance charts required under NYSE and NASD rules, please visit CIBC on the web at http://apps.cibcwm.com/pricecharts/ or write to CIBC World Markets Corp., 425 Lexington Avenue, New York, NY 10017 (212-856-4000) or CIBC world Markets Inc., 161 Bay Street, 4th Floor, Toronto, ON M5H 2S8, Attn: Research Disclosure Chart Request.

Legal Disclaimer

This report is issued and approved for distribution by (a) in Canada, CIBC World Markets Inc., a member of the Investment Industry Regulatory Organization of Canada ("IIROC"), the Toronto Stock Exchange, the TSX Venture Exchange and a Member of the Canadian Investor Protection Fund, (b) in the United Kingdom, CIBC World Markets plc, is Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority, (c) in Australia to wholesale clients only, CIBC Australia Ltd, a company regulated by the ASIC with AFSL license number 240603 and ACN 000 067 256, and (d) in Japan, CIBC World Markets (Japan) Inc., a registered Type 1 Financial product provider with the registration number Director General of Kanto Finance Bureau #218 (collectively, "CIBC World Markets") and (e) in the United States either by (i) CIBC World Markets Inc. for distribution only to U.S. Major Institutional Investors ("MII") (as such term is defined in SEC Rule 15a-6) or (ii) CIBC World Markets Corp., a member of the Financial Industry Regulatory Authority ("FINRA"). U.S. MIIs receiving this report from CIBC World Markets Inc. (the Canadian broker-dealer) are required to effect transactions (other than negotiating their terms) in securities discussed in the report through CIBC World Markets Corp. (the U.S. broker-dealer). CIBC World Markets Corp. accepts responsibility for the content of this research report.

This report is provided, for informational purposes only, to institutional investor and retail clients of CIBC World Markets in Canada, and does not constitute an offer or solicitation to buy or sell any securities discussed herein in any jurisdiction where such offer or solicitation would be prohibited. This document and any of the products and information contained herein are not intended for the use of Retail investors in the United Kingdom. Such investors will not be able to enter into agreements or purchase products mentioned herein from CIBC World Markets plc. The comments and views expressed in this document are meant for the general interests of wholesale clients of CIBC Australia Ltd.

This report has been prepared by the CIBC group and is issued in Hong Kong by Canadian Imperial Bank of Commerce, Hong Kong Branch, a registered institution under the Securities and Futures Ordinance, Cap 571 (the "SFO"). This report is intended for "professional investors" only (within the meaning of the SFO) and has been prepared for general circulation and does not take into account the objectives, financial situation or needs of any recipient. Any recipient in Hong Kong who has any questions or requires further information on any matter arising from or relating to this report should contact Canadian Imperial Bank of Commerce, Hong Kong Branch at Suite 3602, Cheung Kong Centre, 2 Queen's Road Central, Hong Kong (telephone number: +852 2841 6111). Orders for Hong Kong listed securities will be executed by Canadian Imperial Bank of Commerce, Hong Kong Branch. Canadian Imperial Bank of Commerce, Hong Kong Branch has entered into an arrangement with its broker-dealer affiliates worldwide to execute orders for securities listed outside of Hong Kong for Hong Kong clients.

This report is intended for distribution in Singapore solely to "institutional investors" (within the meanings of the Financial Advisers Act (Chapter 110 of Singapore)).

The securities mentioned in this report may not be suitable for all types of investors. This report does not take into account the investment objectives, financial situation or specific needs of any particular client of CIBC World Markets. Recipients should consider this report as only a single factor in making an investment decision and should not rely solely on investment recommendations contained herein, if any, as a substitution for the exercise of independent judgment of the merits and risks of investments. The analyst writing the report is not a person or company with actual, implied or apparent authority to act on behalf of any issuer mentioned in the report. Before making an investment decision with respect to any security recommended in this report, the recipient should consider whether such recommendation is appropriate given the recipient's particular investment needs, objectives and financial circumstances. CIBC World Markets suggests that, prior to acting on any of the recommendations herein, Canadian retail clients of CIBC World Markets contact one of our client advisers in your jurisdiction to discuss your particular circumstances. Non-client recipients of this report who are not institutional investor clients of CIBC World Markets should consult with an independent financial advisor prior to making any investment decision based on this report or for any necessary explanation of its contents. CIBC World Markets will not treat non-client recipients as its clients solely by virtue of their receiving this report.

Past performance is not a guarantee of future results, and no representation or warranty, express or implied, is made regarding future performance of any security mentioned in this report. The price of the securities mentioned in this report and the income they produce may fluctuate and/or be adversely affected by exchange rates, and investors may realize losses on investments in such securities, including the loss of investment principal. CIBC World Markets accepts no liability for any loss arising from the use of information contained in this report, except to the extent that liability may arise under specific statutes or regulations applicable to CIBC World Markets.

Information, opinions and statistical data contained in this report were obtained or derived from sources believed to be reliable, but CIBC World Markets does not represent that any such information, opinion or statistical data is accurate or complete (with the exception of information contained in the Important Disclosures section of this report provided by CIBC World Markets or individual research analysts), and they should not be relied upon as such. All estimates, opinions and recommendations expressed herein constitute judgments as of the date of this report and are subject to change without notice.

Nothing in this report constitutes legal, accounting or tax advice. Since the levels and bases of taxation can change,

Legal Disclaimer (Continued)

any reference in this report to the impact of taxation should not be construed as offering tax advice on the tax consequences of investments. As with any investment having potential tax implications, clients should consult with their own independent tax adviser.

This report may provide addresses of, or contain hyperlinks to, Internet web sites. CIBC World Markets has not reviewed the linked Internet web site of any third party and takes no responsibility for the contents thereof. Each such address or hyperlink is provided solely for the recipient's convenience and information, and the content of linked third party web sites is not in any way incorporated into this document. Recipients who choose to access such third-party web sites or follow such hyperlinks do so at their own risk.

Although each company issuing this report is a wholly owned subsidiary of Canadian Imperial Bank of Commerce ("CIBC"), each is solely responsible for its contractual obligations and commitments, and any securities products offered or recommended to or purchased or sold in any client accounts (i) will not be insured by the Federal Deposit Insurance Corporation ("FDIC"), the Canada Deposit Insurance Corporation or other similar deposit insurance, (ii) will not be deposits or other obligations of CIBC, (iii) will not be endorsed or guaranteed by CIBC, and (iv) will be subject to investment risks, including possible loss of the principal invested. The CIBC trademark is used under license.