ENVIRONMENTAL, SOCIAL AND GOVERNANCE (ESG) REPORT

YEAR ENDED JUNE 30, 2019

BURGUNDY
ASSET MANAGEMENT LTD.

TABLE *of* CONTENTS

ENVIRONMENTAL, SOCIAL *and* GOVERNANCE (ESG) UPDATE: THE YEAR *in* REVIEW

Over the last year, our regional teams have taken initiatives to lead and own environmental, social, and governance (ESG) factors as part of their overall investment research. Engaging with portfolio companies on hardy perennials like cybersecurity, greenhouse gas emissions, and plastic packaging have been among these ESG implementation efforts. New ESG concerns have also surfaced, including employee dissatisfaction and referral marketing. This year, our regional teams used RepRisk, an ESG news aggregation tool, to assist in their ESG research. We have incorporated periodic reviews of the findings at our investment meetings. Below are the highlights from our regional investment teams' ESG work. The body of this report contains a full write-up from each of our regional teams.

ENVIRONMENTAL

Our U.S. Large Cap and European teams engaged with Pepsi and Nestlé, respectively, around various environmental concerns, including both companies' inclusion on the Climate Action 100+ list. Both these companies have retooled their supply chains towards sustainable sourcing practices, and the progress we saw from our engagements has been promising. These efforts have included incorporating more recycled packaging and greater vigilance around suppliers' greenhouse gas emissions. Our emerging market team found a similar commitment to sustainable sourcing from Universal Robina, a Philippine maker of coffee, snacks, and beverages.

On the topic of water usage, our Fixed Income team researched Thames Water Utility. They found the portfolio company is managing its water resources well overall, but needs to make improvements to their leakage controls. The team has since expressed these concerns to management at Thames.

Our investment team continues to monitor the greenhouse gas emissions of its portfolio companies. Our Canadian Large Cap team studied the environmental footprint of natural gas producer Peyto, finding significant reductions in methane emissions, as well as emission intensity of approximately half the industry average. Our Japanese equity team analyzed Suzuki Motor's efforts to reduce the emissions intensity of its cars in India, where it is the largest car maker. We find Suzuki's hybrid/electric vehicle partnership with Toyota is an encouraging start in helping to improve air quality in India.

SOCIAL

Our Canadian and U.S. Small Cap teams focused on the employees of their portfolio companies. To analyze the satisfaction of its portfolio companies' employees, the Canadian Small Cap team used employee review website Glass Door. The differences in company culture and engagement across the portfolio were vast and, at times, surprising. The U.S. Small Cap team concentrated on Primerica's sales agents, who some skeptics claim are being mistreated in a referral marketing structure. The U.S. Small Cap team engaged with Primerica agents as customers, interviewed an agent, and even attended a recruitment meeting. In the end, they found the disparaging claims to be unfounded.

Cybersecurity is another social concern our investment team is carefully observing. We organized cybersecurity risk training for our entire investment team by inviting cybersecurity experts with experience in data breaches to speak in a panel discussion. These experts discussed their experiences working at different major American companies: Target, IBM, and Alcoa (and its spin-off company, Arconic). The full transcript from our session with these experts is available in Appendix B. Our U.S. Large Cap team was able to apply some of these learnings in its research of Equifax. As part of our diligence, Burgundy's IT team also interviewed Equifax's Chief Information Security Officer.

Gender diversity is another social issue our investment department is working on. We recently launched a series of "Women in Investing" programs on university campuses. Led by Robyn Ross, Burgundy's Recruitment and Development Manager, these programs are yielding early signs of success, with more women applying for internship positions at Burgundy and two female interns receiving full-time analyst job offers.

GOVERNANCE

A founding member of the Canadian Coalition for Good Governance (CCGG), Burgundy has been committed to this cause for a long time. Over the last year our regional investment teams engaged with portfolio companies on various corporate governance topics, including shareholder activism, executivecompensation, and headquarter domiciling. A few examples of these engagements are provided in Appendix A.

ESG RATINGS

Our investment team does not use ESG ratings to make decisions. We believe it is our regional teams' job to weigh ESG factors in their decision-making process and come to their own independent ESG judgement. Nevertheless, it is informative to see how our portfolios score on Sustainalytics, the industry-leading ESG rating and research service. As shown below, only two of our geographic strategies can

be evaluated because most of our strategies' holdings are not sufficiently covered by Sustainalytics. Unfortunately, Sustainalytics and other ESG-rating services tend to concentrate on large-cap stocks in developed markets, leaving most of our regional strategies without adequate ratings data. In the U.S. Large Cap and European All Cap mandates, where approximately 90% of the holdings are rated, our portfolios score well. A rating of 99 represents the top one percentile and a score of 50 is average, so both portfolios are well above average.

Our portfolios' above-average ratings are not a result of our investment team targeting high ratings. In fact, no one on our research team regularly looks at these ratings. Rather, the ratings are the output of our deep, bottom-up research process, which seeks quality businesses run by principled managers and which incorporates ESG factors alongside all other investment considerations.

SUSTAINALYTICS RATINGS ANALYSIS

Regional Strategy	Average ESG Ranking	% of the Portfolio Rated
Sufficient Ratings Coverage (>50% of Portfolio)		
U.S. (Large Cap)	60	92% 
Europe (All Cap)	84	88% 
Insufficient Ratings Coverage (<50% of Portfolio)		
Asia (All Cap)		32% 
Canada (All Cap)		40% 
Canada (Small Cap)		0% 
Emerging Market (All Cap)		11% 
U.S. (Small / Mid Cap)		17% 

Source: Bloomberg, Sustainalytics

Doug Winslow
Vice President,
Portfolio Manager

U.S. LARGE CAP CASE STUDY: PEPSICO

SUSTAINABLE SOURCING

PepsiCo is a leading worldwide manufacturer and distributor of packaged snacks, foods, and beverages. The company sells to customers in more than 200 countries with an operational footprint that spans the sourcing of materials, the manufacturing and packaging (including glass, aluminum, plastic) of food and beverage products, as well as the transportation of goods and materials throughout the company's global value chain.

In December 2017, PepsiCo was named on a list of 100 companies by Climate Action 100+, an initiative launched in 2017 to ensure the world's largest greenhouse gas (GHG) emitters take action on climate change. The initial 100 companies were selected based on the absolute level of direct and indirect GHG emissions associated with the use of their products. For PepsiCo, indirect GHG emissions would include emissions produced by the farms that supply the company's operations and emissions from post-consumption activities such as waste disposal. While we recognize that PepsiCo's inclusion on this list is to a large degree a function of its size and scale, we agree that PepsiCo has an opportunity and responsibility to reduce its GHG emissions by implementing more sustainable practices throughout its direct and indirect operations. We also recognize that PepsiCo's role as a significant emitter of GHG globally exposes the company to regulatory risks that seek to cap, tax, or otherwise restrict the use of certain fuel types, which could ultimately increase the cost of PepsiCo's operations.

OUR APPROACH

Our primary approach to assessing and monitoring these matters within PepsiCo has consisted of directly engaging with the company and reviewing their "Performance with Purpose" initiative.

PepsiCo's "Performance with Purpose" initiative is the company's commitment to delivering strong financial performance in a way that is responsible and sustainable over time. While this initiative launched in 2006, PepsiCo expanded the initiative in 2016 to

begin targeting, tracking, and disclosing progress towards specific sustainability goals. Notable environmental goals included:

- Reducing absolute GHG emissions across the value chain by at least 20% by 2030
- Designing 100% of packaging to be recyclable, compostable, or biodegradable by 2025
- Achieving zero waste to landfill across all direct operations by 2025

There is direct oversight of the sustainability agenda at the executive level, as well as a distinct Sustainability Office responsible for performance monitoring and reporting integrity of sustainability initiatives.

Our engagement with the company has involved discussions with a Senior Director in charge of Global Environmental Policy, as well as individuals within Investor Relations. Based on these discussions we believe that management is committed to making progress in these areas and is particularly focused on reducing the level of GHG emissions deriving from indirect sources, which account for approximately 92% of PepsiCo's total emissions. One example of this is the use of more recycled content in packaging, particularly in plastics, as the use of plastic packaging is a meaningful contributor to indirect GHG emissions from PepsiCo. Another is the expansion of PepsiCo's Sustainable Farming Program, which establishes a code of sustainable farming principles and continuous assessment practices to reduce the carbon footprint of the company's suppliers. In our view, these initiatives show that management is taking a pragmatic approach to reducing its carbon footprint. We believe that sustainability governance is strong within PepsiCo and management is taking appropriate and proactive steps to reducing its carbon footprint.

Overall, the company appears to be making strong progress towards these goals.

MOVING FORWARD

We need to be vigilant that a large consumer packaged goods company is acting responsibly with regard to environmental practices. We are confident that PepsiCo's management views sustainability as a priority and has made meaningful initial strides towards implementing sustainability into the culture and operations of the company. We will continue to monitor these risks and engage with the company moving forward. ■

We believe that sustainability governance is strong within PepsiCo and management is taking appropriate and proactive steps to reducing its carbon footprint.

Doug Winslow
Vice President,
Portfolio Manager

U.S. LARGE CAP CASE STUDY: EQUIFAX

CYBERSECURITY

Cybersecurity is becoming an increasingly important ESG issue for our portfolio companies. As more and more personal and business information is digitized, the potential financial or geopolitical gain from cyberattacks for bad actors is increasing.

Well-governed companies with strong leadership and risk management practices are more likely to have a better understanding of cybersecurity risks. Moving forward, we will look at who is responsible for security, whether the board and senior management have the necessary skills to deal with cyber threats (and their level of involvement), and whether the company has cybersecurity training programs in place, among other items.

BACKGROUND

We had to learn (or re-learn) some painful lessons with regard to systems and cybersecurity risks with Equifax.

Equifax is one of the world's largest credit agencies. Credit agencies are in the business of collecting, organizing and managing numerous streams of information pertaining to individuals and businesses including credit, financial, public record, and demographic. Equifax's core North American credit bureau provides financial institutions with credit information on consumers that they use to determine whether to extend credit to prospective borrowers. We first purchased shares in Equifax in 2006.

While the company's economic moat was strong with limited competition, we recognized that IT security, infrastructure and systems were areas that presented the greatest risk to the investment. Even though Equifax was performing well financially, we were concerned that the company appeared to be underinvesting in technology and systems relative to other publicly traded competitors. We trimmed the size of the investment but we continued to hold a position in the company.

The company made several other changes and commitments. The company committed to spend an incremental US$1.25 billion on its technology and security systems between 2018 and 2020.

On September 7, 2017, the company announced that it had been the victim of a cyber-attack which had culminated in a data breach that exposed the names, social security numbers, birth dates, addresses, driver's license numbers and tax information for approximately 148 million U.S. consumers, in addition to almost one million other individuals from Canada and the UK.

During our original period of investment, the CEO had, in retrospect, provided incomplete answers (at best) to our questions. We were deeply disappointed by the magnitude of systems and process deficiencies at the company. (We subsequently sold our remaining shares in the company.) While we did well on our original investment in Equifax overall, we realized that we didn't probe deeply enough within the IT organization to properly assess their capabilities, especially in light of other concerns.

NEW INVESTMENT

In December 2018, we hosted a meeting with management to assess the changes made in the wake of the breach.

There was significant turnover at the management level, with the company hiring a new Chief Executive Officer, Chief Information Security Officer (CISO) and Chief Technology Officer, among others. The hiring of Jamil Farshchi as CISO, in particular, was an eye-opener. Mr. Farshchi has a distinguished track record in the world of information security with former employers that include the Los Alamos National Laboratory (where some of the United States' most sensitive national security and nuclear weapon assets are stored), Visa, and Home Depot. At Home Depot, he was the point man in repairing the company's IT security systems following a breach of its payments system.

Management discussed many of the technology initiatives underway at the company. After discussing several technology-related questions and cybersecurity lessons, the company offered us a call with Mr. Farshchi. Following the meeting, Mr. Farshchi and Burgundy's own IT security team held a call in order to discuss some of the lessons learned over the course of his career and share best practices.

The company made several other changes and commitments. The company committed to spend an incremental US$1.25 billion on its technology and security systems between 2018 and 2020 (with that spend largely falling under the purview of Mr. Farshchi). The new CEO also made meaningful changes to the reporting structure, with a direct line from the CISO and CTO to the CEO, demonstrating a commitment to security and taking the first steps towards a security-oriented culture going forward. In addition to these explicit changes, we were also encouraged by a noticeable change in tone from remaining management, signaling a culture change at the top.

Burgundy also consulted several experts to assess whether Equifax could repair its reputation and return to growth. One expert was the Global Head of Risk Decision Systems and External Data at a large multinational bank. The expert noted that he believed that Equifax would likely enjoy an advantage in data security over its competition going forward, owing to its large team of well-pedigreed IT security professionals and substantial systems investment. We also spoke to a lawyer who spent eight years at the Department of Justice, specializing in misconduct by major financial institutions, in

order to understand the potential liability arising from fines administered by various government agencies. The expert highlighted that in determining fines for corporations, the agencies are forced to consider remediation. This expert believed Equifax's actions to date constituted a meaningful response that would be looked upon favourably by the relevant agencies.

Following these discussions and subsequent research, we began to view Equifax's path to rebuild its reputation and return to growth as credible. As such, we re-initiated a small investment in Equifax in December of 2018. We continue to closely monitor the company's progress on systems and security.

Steve Boutin

Senior Vice President,
Portfolio Manager

U.S. SMALL / MID CAP CASE STUDY: PRIMERICA

REFERRAL MARKETING

Primerica is the largest term life insurance provider in the United States. It targets middle income families with household incomes between US$30,000 and US$100,000, which represent about half the households in the United States. We invested in the business in 2011 shortly after Citigroup, its former parent, took it public in 2010. Citigroup was effectively a forced seller at the time, needing to raise capital to shore up its balance sheet following the global financial crisis. The shares have since quintupled in value, with revenue nearly doubling and earnings per share quadrupling over our holding period.

Despite Primerica's sustained success, it has been the subject of controversy due to its rather unusual distribution model. Primerica uses a sales force comprised of over 130,000 sales agents who are licensed to sell Primerica's insurance and investment products. The agents are considered independent contractors, effectively running their own businesses as distributors of Primerica's products, earning commissions based on their levels of sales. They are also incentivized to convince new representatives to join Primerica's network, as they get paid a cut from the commissions earned by any new agents they recruit. Most agents work this job part-time to supplement the income from their primary employment.

Primerica therefore has a multi-tiered sales force, sometimes called a "multi-level marketing" strategy or "referral marketing" strategy. As such, it is sometimes mistaken for an illegal pyramid scheme, but the nefarious elements of pyramid schemes are all absent from Primerica's model. First, there is no requirement for sales agents to purchase Primerica's products, nor is there any need for them to buy and hold any inventory. Second, the cost to a new agent of joining Primerica's network is low, consisting typically of a one-time US$99 licensing fee to cover an insurance licensing program and a US$25 monthly support fee, on which Primerica earns no profit. Whereas the hallmark of pyramid schemes is that they make money primarily by selling the right to participate in their scheme, Primerica's profits are driven entirely by the sale of insurance policies to end-customers.

We followed up our initial diligence with many direct engagements with Primerica's management over the years, which have affirmed our conviction in the business.

This sales model affords Primerica a lower-cost distribution model than most of its peers, allowing them to offer affordable term life insurance to historically underserved markets. Whereas Primerica focuses exclusively on term life rather than whole life insurance, most insurance companies favour their whole life insurance businesses, which generate higher premiums (and are less attainable for middle-income households) and higher sales commissions. Its policies also boast a better lapse rate over time than the industry average, indicating their real utility to policyholders.

Primerica is also criticized for its high rate of sales agent turnover. Approximately 43,000 licensed agents, or roughly one-third of its total licensed agents, left the network in 2018 and were replaced by roughly 48,000 newly licensed recruits. These newly licensed recruits came from a pool of 290,000 new recruits, of whom less than one-fifth received their license. Although turnover is high, the reality is that most new recruits approach Primerica as a side gig intended to supplement their household income. The low initial cost of joining provides flexibility to experiment with the role before making a bigger commitment. The licensing process, which involves passing an exam, serves as both an important training and screening tool for selecting dedicated candidates. Over 26,000 of Primerica's independent agents have been with the company for more than 10 years, and over 10,000 have been with Primerica for more than 20 years. Those who distinguish themselves with strong performance have the opportunity to become Regional Vice Presidents, a full-time employment role with responsibility for supervising field activity and screening and approving recruits. Overall, the average agent earns over US$6,000 per year in supplemental income with Primerica.

Prior to initiating our position with Primerica, we engaged directly with Primerica sales agents as prospective customers so that we would understand the sales process from start to finish. Our primary contact was a chemical engineer who had quit his engineering career to work with Primerica full-time after experimenting with it on a part-time basis. We attended a recruitment meeting and ultimately purchased a term life policy. The process was entirely straightforward and transparent.

We followed up our initial diligence with many direct engagements with Primerica's management over the years, which have affirmed our conviction in the business.

Kenneth Broekaert
Senior Vice President,
Portfolio Manager

EUROPE CASE STUDY: NESTLÉ

SUSTAINABLE SOURCING AND OTHER ESG TOPICS

Nestlé has been a core holding in the European Equity Fund since 2000. The company's long-term orientation has been an important component of our investment thesis on Nestlé. We believe that this orientation has been a key driver of the excellent returns that it has generated for shareholders during our holding period. In our view, it also makes the company particularly attuned to ESG issues. Due to its size, geographic reach, and the nature of the categories that it is present in, Nestlé's actions on ESG have a greater absolute impact on society than any other company in the European portfolio. Nestlé is the 13th largest company in the world by market capitalization and the second largest manufacturer in the world. It is present in 190 countries and is a leader in categories with major societal significance, such as products targeting infants and child nutrition. We believe that Nestlé is a clear global leader on ESG issues. Below we outline Nestlé's approach to ESG, highlight some of its successes in this area, and describe recent interactions that we have had with the company on ESG.

ESG is deeply integrated into Nestlé's corporate strategy, which is predicated on the premise that "business results and positive societal impact should be mutually reinforcing" and that "to be successful in the long term, value must be created for both shareholders and society." The company believes that shareholder value is not sustainable over the long term if it is created at the expense of other stakeholders. We wholeheartedly agree with and support this approach.

Nestlé's approach to ESG goes well beyond platitudes. It sets specific and measureable goals across 17 ESG categories and reports on its progress against these goals annually. While Nestlé's goals span all aspects of ESG, it places particular emphasis on child and societal nutrition because it has a leading presence in nutrition around the world and, as a result, believes that its efforts here will yield more productive results for society than if focused on other areas of ESG. Through its emphasis on nutrition, Nestlé has made significant progress enhancing the nutritional quality of its food, improving the availability and affordability of nutritional food to vulnerable communities, and increasing awareness of the importance of healthy eating. Some of Nestlé's key

ESG is deeply integrated into Nestlé's corporate strategy, which is predicated on the premise that 'business results and positive societal impact should be mutually reinforcing' and that 'to be successful in the long term, value must be created for both shareholders and society.'

accomplishments in other areas of ESG in 2018 are a 32% reduction in greenhouse gas emissions per ton of product from its manufacturing operations relative to 2010, a 30% reduction in water usage per ton of product relative to 2010, and a global workforce with 43% of the company's senior leadership roles held by women.

Nestlé also supports ESG issues by being actively involved, often in a leadership role, with non-governmental organizations that advocate for businesses to adopt sustainable and socially responsible practices. Some of the most important organizations that Nestlé is actively involved with are:

- *The United Nations Global Compact.* The world's largest ESG organization. It encourages businesses to formerly adopt 10 ESG-related principles spanning human rights, labour, the environment and corruption.

- *The Carbon Disclosure Project.* A UK-based, non-governmental organization that advocates and provides a framework for businesses to report on their environmental impact.

- *The Climate Disclosure Standards Board.* A non-profit organization working toward the integration of climate change related information into financial reporting.

While we evaluate Nestlé's approach to ESG by our own standards, it is worthwhile to note that the company has been recognized by a number of well-respected organizations for its approach and contribution to ESG issues. The following are some of the most notable:

- The Access to Nutrition Foundation, a non-governmental organization financed by the Bill and Melinda Gates Foundation, ranked Nestlé second out of 22 multinational food companies for its contribution to solving global nutritional challenges.

- The aforementioned Carbon Disclosure Project awarded Nestlé an "A", the organizations highest rating, in recognition of its actions to cut greenhouse gas emissions, mitigate climate risks and develop a low-carbon economy.

- Dow Jones includes Nestlé in its Sustainability Index. The Dow Jones Sustainability Index is comprised of what Dow Jones considers the top 10% of the largest 2500 companies in the world on climate change strategies, energy consumption and corporate governance.

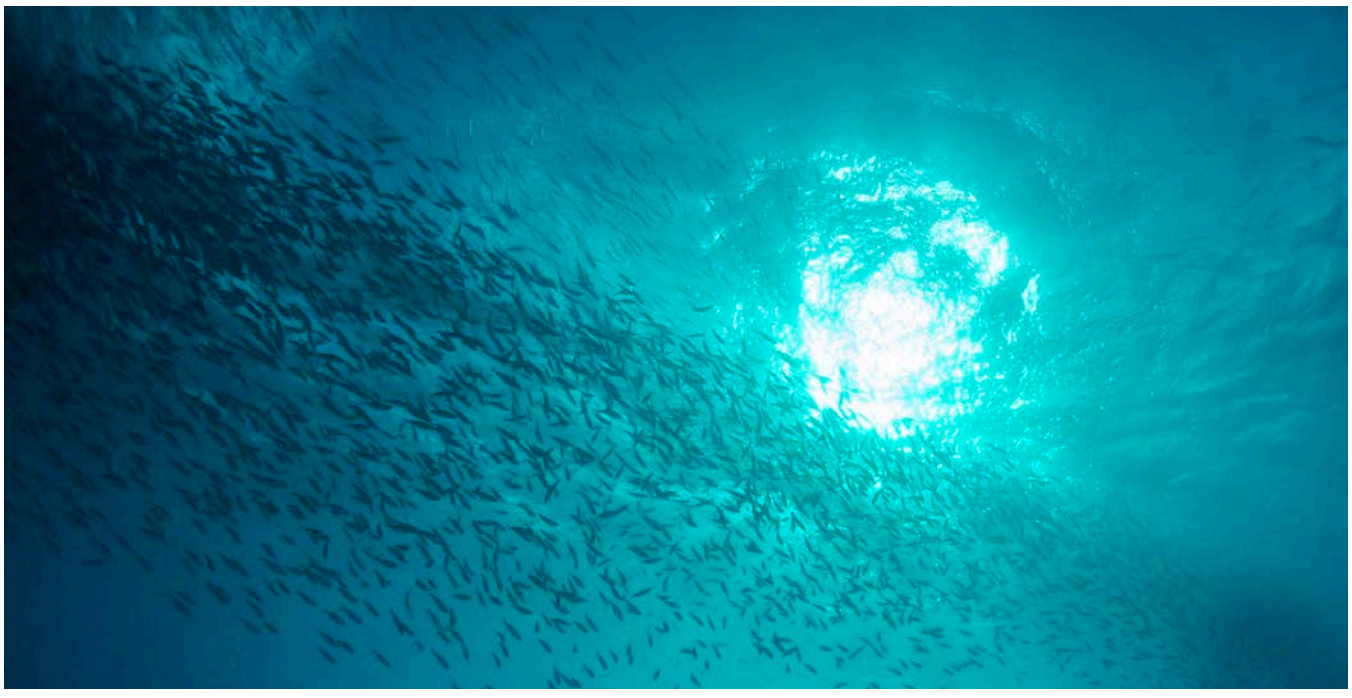
We formally interacted with Nestlé twice over the past 18 months on ESG related issues. In both instances the company provided responses to our enquiries that we felt adequately addressed the issues that we raised, and that were reflective of the importance that Nestlé places on ESG issues. The first issue that we raised with Nestlé was its inclusion in the Climate Action 100+. The Climate Action 100+ is a list of the top 100 greenhouse gas emitters in the world, as determined by a non-profit organization of the same name. Nestlé acknowledged its inclusion in the Climate Action 100+ to us, and noted that it was predominately a function of its size, as the second-largest manufacturer in the world, rather than its environmental practices. Nestlé also directed us to documents that it published on its greenhouse gas emissions. The documents describe Nestlé's approach to reducing greenhouse gas emissions and track the company's progress on it against specific and measurable goals. The documents

also referenced some of the favorable ratings that Nestlé has received on its approach to greenhouse gas emissions from independent non-governmental organizations that evaluate businesses on that issue.

The second interaction that we had with Nestlé on ESG issues was over its identification as a meaningful participant in the global fishery industry (via its pet food business) by the Fish Tracker Initiative. The Fish Tracker Initiative is a non-profit organization that seeks to align capital markets with the sustainable management of fisheries, an industry that is notorious for poor environmental and labour practices. We raised this issue with Nestlé and the company directed us to a document that it published outlining its approach to sustainable fishing. In the document Nestlé notes that a critical first step to ensuring the sustainability of its seafood supplies is tracing the seafood that it purchases back to its original source (farm or boat) and ensuring that they employ sustainable practices. This is particularly challenging for Nestlé because it uses fish by-products in its pet food, which are difficult to trace. Nestlé has made considerable progress in this regard and in 2018 it was able to trace 99% of the seafood that it purchased in that year back to its source. It was also able to confirm that at least 42% of the seafood that it purchased in that year was responsibly sourced. It is taking steps to increase the portion of its seafood purchases that it can confirm are responsibly sourced.

Our own recent interactions with Nestlé's senior management provide some anecdotal evidence of the importance that the company places on ESG issues. We visited Nestlé's senior management at the company's head office in Vevey Switzerland last year. The company's approach to energy conservation was apparent from the moment we arrived. To enter the head office we had to wait, with other visitors, for several minutes in a very small room situated between the main building and the outdoors in order to minimize heat loss in the main building and maximize its energy efficiency. In a subsequent meeting that we had with senior management in early 2019, they began the meeting by informing us that they did not have business cards and explained that the practice had been ended companywide in an effort to reduce waste.

Nestlé's approach to ESG is rooted in a desire to protect the sustainability of the company's earnings power over the long term and is accentuated by a purpose-driven culture that seems to have a genuine passion for ESG issues. It has clearly worked well for shareholders and we believe society as well. ■



David Vanderwood

Senior Vice President,
Portfolio Manager

CANADIAN LARGE CAP CASE STUDY: PEYTO

ENVIRONMENTAL IMPACT

The International Energy Agency forecasts that global demand for energy will increase 27% by 2040. Driven by the displacement of coal and in support of renewable energy development, global demand for natural gas is expected to grow by 43% over the same period. Canada, which is the fifth-largest natural gas producer in the world, is home to an enormous undeveloped resource base and well-regulated, technically advanced natural gas industry, making the country uniquely positioned to play a key role in that future growth.

Peyto Exploration & Development Corp., a long time holding in Burgundy's Canadian equity portfolios, is the fifth-largest natural gas producer in Canada. The company was founded in 1998 with a strategy to enhance shareholder value through the exploration, discovery and low-cost development of oil, natural gas and natural gas liquids in the Western Canadian Sedimentary Basin. The company chose the sweet gas bearing, sandstone resource plays within Alberta's Deep Basin as its resource platform. This platform has remained the company's main focus and is largely responsible for Peyto consistently achieving a record of economically and environmentally sustainable development. The company's operations are executed in a manner that stresses cost control and efficiency which, by its very nature, leads to less land disturbance, more effective water usage and reduced emissions. In short, there is a strong alignment between low-cost, efficient operations and environmental impact minimization.

LAND USE

Land use and footprint minimization are at the forefront on the Peyto design. This is reflected in the careful selection of surface leases and pipeline right-of-ways to minimize forest and ecosystem disturbance.

Peyto's philosophies and practices surrounding major facility development are consistent with land disturbance minimization. The company constructs compact, modular

facilities that are “right-sized” and expandable with the resource development and production growth. This ensures minimal land use per unit of energy produced while simultaneously minimizing fuel consumption and fuel-related emissions.

Wellsite footprints are getting smaller over time on both a well and unit of production basis. When practical, Peyto uses small single-lease footprints to host many wellbores of different depths and geological formations. This reduces capital requirements for lease construction, equipping and pipelining while placing four or more wells on a space that traditionally hosted only a single well. It also contributes favourably to the reduction in disturbance and emissions.

EFFECTIVE WATER USE

Peyto has a stated goal to practice effective water management by increasing the volume of recycled water and decreasing the fraction of freshwater make-up used in the hydraulic fracture stimulation operations.

Each well development carries its own unique attributes with respect to water management, requiring customized water sourcing, storage, disposal and recycling strategies. When considering these elements, Peyto considers not only cost impacts but also any environmental impacts and regulatory requirements associated with all available sourcing options. These sourcing options can include ground water, surface water, saline produced water, recycled flowback water and recycling initiatives of non-potable alternative sources. In most situations, a combination of these sources is combined into a customized strategy unique to each given well or pad.

A recent upstream oil and gas water use report issued by the Alberta Energy Regulator (AER) noted that industry water used for hydraulic fracturing was made up of only 6% recycled water and an additional 1% of alternative water, leaving 93% being supplied by non-recycled sources. In comparison, more than 30% of the water used by Peyto is recycled.

GREENHOUSE GAS (GHG) EMISSION INTENSITY

Peyto has a stated goal to reduce the methane component of its GHG emission intensity by 50% or more from 2013 levels. The company is well on its way to meeting this target. Since 2013, Peyto has already reduced the methane component of its GHG emission intensity by 44%.

The company’s major sources of methane emissions are their wellsite controllers and their wellsite methanol pumps, both of which vent a small volume of methane as part of their normal operational functionality. Peyto has trialed several zero emissions electrical pumps powered by solar electricity and have moved into implementation of this new style of equipment. As they drill and equip new wells with this new equipment over the next several years, the company expects to achieve its goal of a 50% reduction in methane emission intensity.

Peyto’s focus on efficiency is clearly evident when compared to the broader natural gas production and processing industry in Canada. In 2016, the last year that industry-wide data is available, the natural gas sector average greenhouse gas emissions intensity in western Canada was 43.0 kgCO2eq/barrel. By way of comparison, Peyto’s emissions intensity was only 23.9 kgCO2eq/barrel in 2016. The company continues to improve, with emissions intensity dropping to 21.0 kgCO2eq/barrel in 2018, or less than half of the industry average.

In short, there is a strong alignment between low-cost, efficient operations and environmental impact minimization.

Andrew Iu
Vice President,
Portfolio Manager,
Director of Research

CANADIAN SMALL CAP CASE STUDY:

HOSTELWORLD AND HÉROUX-DEVTEK

EMPLOYEE SATISFACTION

At its core, ESG is a stakeholder framework which poses the question: How well does the company balance the competing priorities of different stakeholders? A crucial stakeholder of every company is its employees. Companies with high employee satisfaction tend to outperform because they avoid the implicit costs of employee turnover, employee sabotage, and other ills.

For many years, Burgundy's investment team has interviewed ex-employees of companies to improve its understanding of employee satisfaction and corporate culture, among other reasons. In an effort to systematically understand employee satisfaction at its portfolio companies, the Canadian Small Cap team recently undertook an analysis of its portfolio companies' Glass Door ratings and reviews.

Glass Door is an anonymous website where employees, past and present, can leave reviews and ratings about their employer. Because the site is anonymous, employees write what they really feel, offering a window into employees' day-to-day lives and, more broadly, the company's culture. Every company has some disgruntled employees, so no individual review can be taken as representative. However, with a large enough sample of reviews, interesting patterns sometimes emerge.

Below is a sample of reviews written about two Canadian Small Cap holdings: Hostelworld and Héroux-Devtek. Hostelworld had the highest corporate culture rating on Glass Door in our portfolio, while Héroux-Devtek was near the bottom.

HOSTELWORLD

"The people are what make this place great! Hostelworld is also a really strong brand that is doing good things by connecting travellers all over the world. You can feel how passionate everyone is about this, and we expect great things with a new vision and leadership team on board."

"Good benefits - health insurance, pension, free lunches and snacks, taxsaver scheme. Atmosphere - monthly social events plus last Friday drinks and pizza in the office, cake for birthdays etc., people are nice in general. Office - The office itself is really nice and open."

"New CEO and Executive Leadership Team are really strong and are making all of the right changes in the business. Great at bringing colleagues on the journey with them. Comms has improved with monthly Town halls and ELT are very transparent and honest when answering questions. Great culture & people - everyone is super passionate about travel and hostels, really encouraging and inclusive and great teamwork."

"Great office environment. Excellent monthly events to keep you going and keep a positive environment. I have amazing support from my Manager who invests in my growth. Very fun office space, but hard-working environment at the same time."

HÉROUX-DEVTEK

"Take everything not nice to say about this place and put it in this box. If you are lucky, they will look past you and act like you don't exist. And that is only if you are lucky."

"Management/supervision is terrible, just terrible. Very disrespectful. Unrealistic time commitment expectations. Atmosphere is very combative. They don't understand the processes that they oversee, then complain of poor quality, all the while ignoring helpful suggestions from experienced people. Pay is below average, raises are non-existent, benefits are poor and overpriced. Everyone is overworked to the point of burnout. Hope you don't value your weekends or nights or holidays because you'll be expected to work most/all of those."

"Long hours and unreasonable workload, low pay. They hire in people with experience to clean up messes, and as soon as they are caught up, they let them go. Someone else mentioned unethical, and I would have to agree. They don't appreciate their employees, especially if you are not Canadian. To them, everyone is expendable so the turnover is high, and when half the company is new at their jobs, it is very difficult to run smoothly. People are fighting all the time because they are overworked and burned out. I was told the job was flexible and had plenty of time off, but there were so many restrictions you could never take it."

"Upper management is only worried about looking good. They make sure they take all the credit when something goes right and have plenty of people to blame when things go wrong. They lie to every hire. Don't expect to do the job they describe, or have any say in how anything will be done. They want you so they can blame their mistakes on you."

Of course, both of these companies had some employees who left positive comments and some who left negative comments, but on balance, Hostelworld's culture is described as engaging and dynamic while Heroux's is described as suffocating and internecine. These reviews were one reason that we recently sold Héroux-Devtek. While the main reason was our concern around capital misallocation (Heroux had recently leveraged its balance sheet to finance a major acquisition), employee reviews like the above were also a factor in our decision making process.

Companies with high employee satisfaction tend to outperform because they avoid the implicit costs of employee turnover, employee sabotage, and other ills.

Craig Pho
Senior Vice President,
Portfolio Manager

ASIA CASE STUDY:

SUZUKI MOTORS

CARBON EMISSIONS

One portfolio holding for which ESG is a real business concern and on which we have engaged with management is Suzuki Motors (Suzuki). Suzuki owns 56% of its publicly listed subsidiary Maruti Suzuki (Maruti), the dominant car company in India with about 50% share in the passenger vehicle market.

Low air quality caused by pollutants is a major social health issue in India today. According to the 2018 World Air Quality Report by Greenpeace, India is home to 22 out of the world's 30 most polluted cities[1]. There are many contributors to India's air pollution issue including its reliance on coal-fired electrical plants (which are far more harmful for the environment than more advanced U.S. or Chinese coal plants[2]) and the still-common practice of burning garbage, but undoubtedly passenger vehicle emissions are an important one.

With over four million vehicles produced (over three million of which are sold domestically), India is the world's fourth-largest car market, larger than Germany and behind China, the U.S., and Japan[3]. Of this, Maruti produced over 1.78 million vehicles in its most recent fiscal year, making it the largest automaker in India by a wide margin. As a result, Maruti is also likely the largest contributor in its industry to total Indian CO2 emissions, and the company has an important leadership role to play in improving the Indian environment by increasing the fuel efficiency of its vehicles.

Due to the parent company Suzuki's roots as a company specializing in "mini" vehicles in Japan and its resulting expertise in small internal combustion engine (ICE) technology, Maruti has a strong track record of producing fuel efficient vehicles. For instance, Maruti offers both the number one and number two most fuel efficient passenger vehicles in India[4]. More importantly, however, the trend towards greater fuel efficiency is continuing: The company's average CO2 emissions per passenger car in India have declined 9% since 2012[5].

> By doing so the company will not only comply with government standards but also maintain its positioning as an auto industry leader in India that offers consumers what they want.

Despite already offering several of India's most fuel efficient cars, Maruti needs to further improve its emissions technology in order to help contribute to addressing the pollution issue in India. What's more, the Indian government is continually increasing environmental regulations by creating aggressive future targets for emissions reduction. For instance, Prime Minister Modi's government has set a target of electric vehicles making up 30% of new sales of cars and two-wheelers by 2030, up from less than 1% currently[6]. In order to help adoption, the government recently approved the "Faster Adoption and Manufacturing of Hybrid and Electric Vehicles" (FAME) scheme, under which electric vehicles under 1.5 million Indian rupees will be eligible for subsidies. As a result, in the future Maruti will need to not only offer fuel efficient ICE options for consumers, but also work towards offering vehicles with different engine technologies altogether like electronic vehicles and hybrids.

With the above in mind we are well aware that continually improving its emissions technology is critical to the viability of Maruti's business, and have discussed future investments into emissions reduction technologies with Suzuki. Most notably, in November 2017 the company concluded a memorandum of understanding with Toyota Motor Corporation to move towards a cooperative structure for introducing EVs in India around 2020. What's more, the two companies have also recently made an agreement under which Toyota provides its hybrid engine technology to Suzuki in exchange for cooperation in the Indian market. As a pioneer in hybrid engine technology with massive global resources for technology investment, we see Toyota as an ideal partner for Suzuki in this area. Although it is still early days we are optimistic about Maruti's future. We believe that through its parent Suzuki, Maruti will have access to the necessary technology to continue to improve the fuel efficiency of its products in India. By doing so the company will not only comply with government standards but also maintain its positioning as an auto industry leader in India that offers consumers what they want.

[1] **Source:** https://asia.nikkei.com/Spotlight/Environment/India-home-to-22-of-30-most-polluted-cities-in-the-world-report

[2] **Source:** https://economictimes.indiatimes.com/industry/indl-goods/svs/metals-mining/indias-coal-power-plants-unhealthiest-in-world-study/articleshow/68092797.cms

[3] **Source:** https://economictimes.indiatimes.com/industry/auto/india-pips-germany-ranks-4th-largest-auto-market-now/articleshow/63438236.cms

[4] **Sources:** https://www.autocarindia.com/car-news/top-10-fuel-efficient-automatic-cars-in-india-406827; https://www.carblogindia.com/best-mileage-cars-in-india/

[5] **Source:** 2018 Suzuki CSR & Environmental Report

[6] **Source:** https://www.hindustantimes.com/business-news/india-s-electric-vehicle-goals-being-realised-on-two-wheels-not-four/story-nJxQln7WyuGqH5TMcj7ZAL.html

Anne Mette de Place Filippini

Senior Vice President,
Deputy Chief Investment
Officer and Portfolio Manager

EMERGING MARKETS CASE STUDY:

UNIVERSAL ROBINA

SUSTAINABLE SOURCING

Universal Robina Corporation (URC), listed in the Philippines, is a food and beverage company controlled by the Gokongwei family. In addition to strong market position in its home market of the Philippines, URC's operations extend to Thailand, Indonesia, Vietnam, New Zealand and Australia. As a food and beverage company, URC sells branded products in the instant coffee, salty snacks, biscuits, non-carbonated beverage categories. These products require natural resources and labour to produce, contain salt and sugar, and produce a lot of residual (typically plastic) waste.

It is important to recognize that when it comes to sustainability, emerging market companies are usually laggards compared to developed-world companies. Emerging market companies have to compete with small regional competitors who do not always follow the laws (regulatory, labour etc.) resulting in unfair competition.

URC has shown leadership by publishing a sustainability report in 2016. For this report, URC engaged all stakeholders so that it could demarcate its objectives. URC disclosed five areas of focus: (1) Natural Resources, (2) People, (3) Product, (4) Supply Chain, and (5) Economic. In order to establish some clear objectives, the company benchmarked its performance on these parameters with global peers. URC has now defined key performance indicators in each of its focus areas in order to measure its progress.

URC requires natural resources for almost all of its products. The company is embarking on a multi-pronged journey in order to manage its impact on the environment. For its recycling initiatives, URC has already started to recycle the waste material produced into bio-gas as well as electricity. For its sourcing needs, URC intends to source materials from organizations that are certified suitable. This is especially applicable to their palm oil purchases. Importantly, for water use, URC follows: Reduce, Reuse, and Recycle. While the amount of water URC recycles is low at present (about 10%), efforts are on to make sure this number rises in the future or alternative uses can be found for the waste water.

Another illustration of URC's sustainability agenda is its focus on people. This is another example of a social concern which is more prevalent in emerging than developed markets. URC not only cares about the wellbeing and development of its employees, but is putting programs in place to make sure that their partners are succeeding. URC sources some its key raw materials from farmers and considers it a duty to educate these farmers on best farming practices so that they can create win-win scenarios.

While quality is taken for granted in the West due to strong regulatory environments, the situation in emerging markets is different. Good companies have to have robust processes in order to track supply chains with various quality-assurance checkpoints. This ensures that only a safe product reaches the customer. Increasingly, URC has been changing its portfolio in order to introduce healthier options. It partnered with Danone to introduce water-based beverages and with Vitasoy to introduce plant-based (soy) beverages. These products have much lower sugar levels compared to the established products. URC is also working with its peers as well as other organizations in order to figure out ways to reduce plastic waste. So far, progress on this initiative has been slow.

We believe this focus on sustainability shows URC's commitment to nurture the business for the long term. This aligns well with Burgundy's investment philosophy. Furthermore, this commitment also reveals the culture that the management is trying to foster at URC. At Burgundy, we believe a management and a controlling family who are interested in the betterment of all stakeholders will take the interests of the shareholders very seriously.

URC not only cares about the wellbeing and development of its employees, but is putting programs in place to make sure that their partners are succeeding.

Vincent Hunt
Vice President,
Portfolio Manager

James Arnold
Vice President,
Portfolio Manager

FIXED INCOME CASE STUDY:

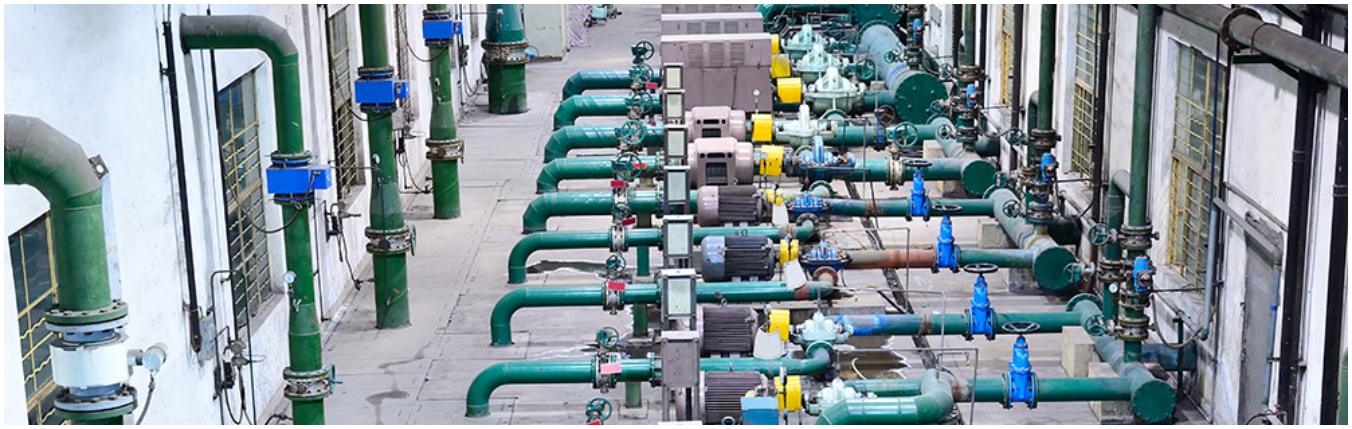
THAMES WATER UTILITY

VARIOUS ESG TOPICS

Thames Water Utilities Finance Ltd. (Thames) provides water and wastewater services in the Greater London Area and the Southern United Kingdom. As a public water utility that delivers an essential service, Environmental and Social Responsibility are important to Thames. In addition, a focus on Governance has become a top priority in the last few years. Showcasing their dedication to these issues, Thames began publishing an Environmental, Social and Governance Statement in 2018. This is in addition to their Corporate Responsibility and Sustainability Report that was already being published annually.

The increased focus on Governance in recent years has led to a number of positive changes at Thames. The Board of Directors has been a significant focus as evidenced through the appointment of a new, independent Chairman of the Board of Directors in January 2018. A pledge was also made to increase, above 50%, the proportion of independent directors. Currently, 46% of the directors at Thames are independent, an increase from 36% in 2017. In an effort to increase transparency and decrease confusion within the corporate structure, management has also opted to remove the Cayman Islands-based subsidiaries. Additionally, Thames implemented a new dividend policy aimed at reducing dividends going forward to allow for increased investment in the water infrastructure.

As a public utility, Thames is committed to the betterment of the individuals and communities they serve. They strive to accomplish this through numerous social programs, both for their employees' wellbeing and the wellbeing of the broader community. Their community initiatives include programs for customers in need, which provide discounted services. Need is not necessarily defined only by financial circumstances but other circumstances as well. For example, reliance on water for dialysis treatment would qualify. Thames is active in schools as well, offering programs to engage children on key topics such as water conservation and preventing sewer abuse. Schools can also participate in tours at various facilities, bring in speakers for their classes or access free educational resources on the company website. The company is also committed to



improving their pipes, rehabilitating over 8,000 lead water pipes since April 2018, making their network safer for the community.

Given that Thames is a supplier of drinking water and also treats wastewater, the environment has always been a top priority. Thames is always striving to improve their treatment of the environment, as indicated by the following stats:

- 70% reduction in pollution incidents since 2013.
- Approximately 25% of power used in the pumping of water throughout the system is self-generated in the sewage treatment process and 100% of power used is from renewable sources.
- 99.96% compliance with drinking water standards – this has been consistent over the past three years.
- 99.43% compliance with Wastewater Treatment Works Discharge Standards, this is up from 98.28% in 2017.

While Thames is performing well in many areas, one issue that we have engaged with management on in significant detail is leakage within the water delivery infrastructure. Thames has missed their leakage target in each of the past three years and has been fined accordingly by their regulator. As such, they are incented to deal with this issue as the fines can be substantial, particularly for a regulated entity. Thames is increasingly dedicating resources to finding and preventing leaks. This includes a number of initiatives such as: having teams on the ground searching for leaks and using data analysis, acoustic devices and thermal imaging. There is an increased likelihood of leakage associated with extreme weather events such as freeze/thaw cycles and heat waves. Given the increasing occurrence of these extreme weather events, it is expected that reaching leakage targets will continue to be challenging for Thames. While we recognize that management is committing significant resources to this, we will continue to monitor leakage numbers going forward.

As a public utility, Thames is committed to the betterment of the individuals and communities they serve. They strive to accomplish this through numerous social programs, both for their employees' wellbeing and the wellbeing of the broader community.

GENDER DIVERSITY *on* BURGUNDY'S INVESTMENT TEAM

GENDER DIVERSITY DISCUSSION

Women are woefully underrepresented in the finance industry. Fewer than one in five CFA members are women and, based upon our analyst recruiting experience, women are even rarer in the investment analyst community. When we launched an intern program three years ago, we were saddened to see the same pattern emerge in undergraduates, with women sometimes accounting for less than 10% of our intern applicants.

In response, Burgundy commissioned a student-run consulting group to help us understand why so few women were applying for finance internship positions. The study was eye-opening, revealing concerns ranging from intimidating job descriptions and interview questions, to aggressive industry culture, poor work/life balance, uneven access to career information and mentorships, and myopic work.

Clearly, the finance industry has a perception problem among women. Two years ago, we launched a "Women in Investing" university program to help change this. The program is run by Burgundy's past female interns and involves these volunteers organizing book clubs and seminars to teach other female students about the kind of quality-value investing that Burgundy practices. The program also involves Burgundy's investment team travelling to campuses to host seminars for participating female students.

We have also improved some of our other recruiting practices. Over the past two years, we have sponsored and spoken at women-focused student conferences, revisited our job postings to remove unintended biases, and posted an interview preparation package on our website in an attempt to "level the playing field." (From the consulting project, we learned that male students sometimes get the interview questions ahead of job interviews from their male mentors.) We also started speaking to female high school students before they start undergraduate business programs to encourage them to consider finance as a career stream.

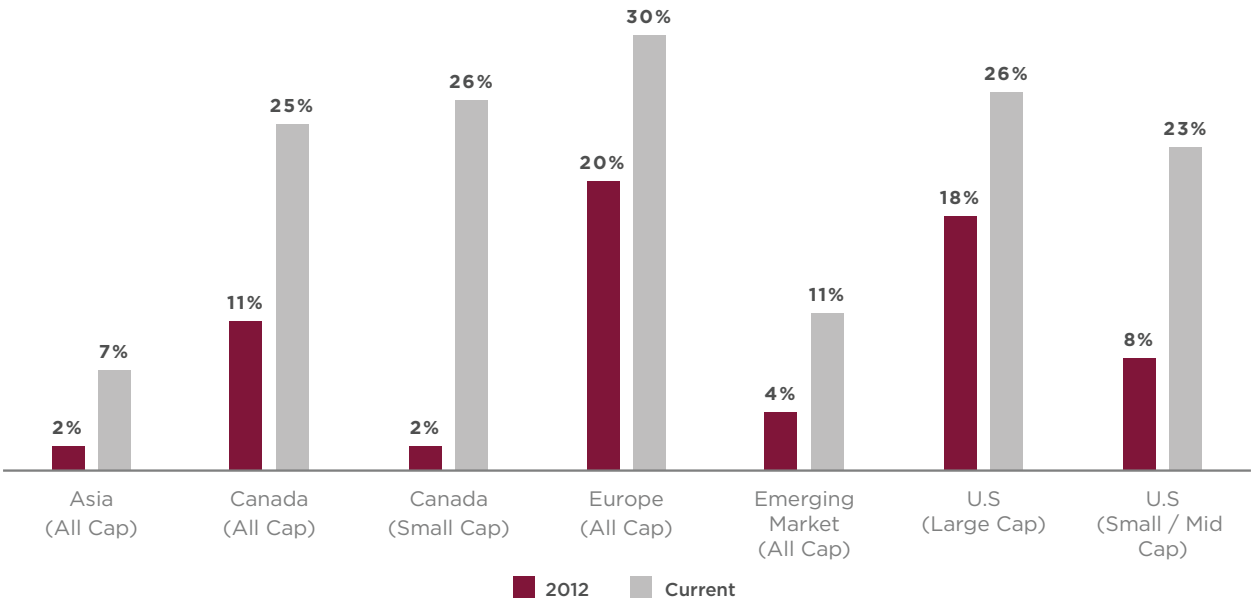
Two years ago, we launched a "Women in Investing" university program to help change this. The program is run by Burgundy's past female interns and involves these volunteers organizing book clubs and seminars to teach other female students about the kind of quality-value investing that Burgundy practices.

Through these initiatives, we have reached over 300 young women and are beginning to see some small but encouraging signs of change. Of our most recent intern applicant pool, one-quarter was female – a major improvement. Over the last year, four of our 10 interns were women. More importantly, we extended job offers to two of these women to join our investment team on a full-time basis. Both of these young women were outstanding interns, demonstrating skills, tenacity, and talent which rivalled some of our full-time analysts. While we recognize that these hires are only two small victories, and change will take many years, we are excited about the prospect of raising the bar for research excellence by attracting the best and brightest young women to our investment team.

GENDER DIVERSITY IN BURGUNDY'S EQUITY PORTFOLIOS

What about gender diversity at Burgundy's portfolio companies? We are seeing early progress here as well. Below is the average percentage of the board of directors that is female in our main geographic strategies. Across all geographies, we are seeing an improvement. While showing the lowest percentage of women in an absolute sense, Asia and the Emerging Markets have witnessed large percentage gains. Europe is the leader, with nearly one-third of our European companies' boards composed of women, while North America sits in the middle with roughly one-quarter of North American boards composed of women.

WOMEN AS A PERCENTAGE OF THE BOARD OF DIRECTORS



Source: Bloomberg, as of June 30, 2019

APPENDIX A

EXAMPLES *of* GOVERNANCE ENGAGEMENTS

Company	Engagement Detail	Method of Engagement	Outcome
BB&T Corp	Efficacy of IT and cybersecurity risk.	Company meetings.	The company appears to be approaching the issue thoughtfully and appropriately.
Equifax	Efficacy of IT and cybersecurity risk.	Company meetings.	The company appears to be approaching the issue thoughtfully and appropriately.
Nestlé SA	Amid pressure from an activist investor, we conveyed to the CEO that we are not supportive of particular initiatives suggested by the activist that could have a positive impact on the share price in the short term, but negative consequences for the business over the long term. We emphasized to the CEO that we are supportive of his long-term approach to the management of the company.	Company meeting.	We are confident that management will not acquiesce to activist requests that are not in the long-term interest of the company.
Oracle Corp	Magnitude of executive compensation.	Conference call with investor relations. Voted against "say on pay" provision in the proxy.	The company is making changes in the right direction but more work needs to be done.
Sabre Corp	Concern over the quality of certain management, the metrics that executive compensation was based on, and the robustness of the company's IT platform.	Company meetings and written communication.	Ongoing but the company has made significant changes that we are satisfied with.
Unilever NV	Concerned that consolidating the company's head office structure to the Netherlands could degrade corporate governance.	Written communications.	The company abandoned its plan to consolidate its head office structure.

APPENDIX B

EXPERT PANEL TRANSCRIPT: ESG TRAINING MATERIAL *on* CYBERSECURITY *and* DATA PRIVACY

JOANNE MARTIN
Former VP, IT Risk and Global CISO at International Business Machines Corporation

ALAN LEVINE
Former CISO at Arconic Inc.; Global Information Security, Privacy, and Compliance at Alcoa Corporation

BRYAN STRAWSER
Founder, Principal, and CEO at Bryghtpath LLC

BURGUNDY INTERVIEWER: ROBYN ROSS
Recruitment and Development Manager

RR: Over the weekend, I was trying to explain to my seven-year-old and my ten-year-old what mom was going to do on Monday morning. I explained why we do these panels and why we bring in these experts, and my son said to me, "You're really bringing people in to show that you're not smart?" That really sums up the purpose of these panels because the minute we become smart, that's our greatest enemy, especially around data and data privacy. As guardians of our clients' capital, we simultaneously become guardians of their data. We are joined today by Bryan, Joanne, and Alan. They are all experts in this field. I'm going to let them introduce themselves and then we'll have a whole bunch of questions that will dig into data and data privacy.

BS: I'm Bryan Strawser, currently principal and CEO of a consulting firm based in Minneapolis, Minnesota called Bryghtpath. Prior to forming Bryghtpath five years ago, I spent 21 years at Target Corporation, the last six as the head of global crisis management, business continuity and intelligence. I'm also a senior fellow at the Center for Cyber and Homeland Security at George Washington University in Washington, D.C., where my work is really on the intersection between public and private sectors when it comes to cybersecurity and U.S. national security issues.

JM: I'm Joanne Martin. I retired from IBM about four years ago. I was the global CSO and Vice President of IT risk there. I'm doing consulting now, doing CSO as a service for medium-sized businesses. The biggest one I deal with is McCormick Spices in Baltimore. I fit in where they have an absence of security focus. It's an interim role there. I'm on the CSO Coalition. I'm one of the global leaders there with other CSOs who need a place to safely share our concerns and what we are doing about them.

AL: I'm Alan Levine. I'm the former Chief Information Security Officer and Chief Privacy Officer for Alcoa, formerly many years ago known as the Aluminum Company of America before it went global. A couple of years ago Alcoa as we knew it separated into two new Fortune 500s. One retained

the name Alcoa; one took on the name Arconic. I became the CSO and CPO for Arconic until mid-last year when I took my leave. For several years I've been the board chair for Carnegie Mellon University's CSO programs, all of them that we do for private industry and for some DOD and DHS operations as well.

RR: In your careers, you've all been part of or working for companies that have had some serious data breaches. Could each of you set the scene for when a significant data breach happened and the scene leading up to that?

JM: I actually do not have a significant breach. I've had incidents. I'm going to draw a line between a data breach and a data incident, a security incident. I think to my credit, we didn't have a media event around any of our incidents. At IBM we probably had 2-3 open a week at any given time, somewhere in the world. But they didn't hit the press. As a CSO, that's number one: let's keep it out of the press, because then it becomes a reputational issue. How you manage an incident is as important as not having one.

The biggest one we had, the perpetrator ended up going to jail in Europe. His going to jail was a press event, but we weren't associated with it. What led up to: it was a defect in one of our software products. He was able to exploit that. It was a big issue. There was a mix of responsibilities and that's one of the things you have to do quickly when you have an incident is figure out how it happened and how to contain it, whose responsibility it is. This was a mix because IBM's client had some responsibility too for what they had not done and we had to sort that through. Once we did and we knew what the problem was, we also had to put out a patch in December to all of our clients around the world, telling them not to ask what it was for, but to please trust us and to put a patch on their systems – even if you're a bank or a retail company, but it really needs to go in now. Our biggest challenge was to roll that patch out and make sure everybody got it put in place. Because, of course, once anything had been exploited it was extra bad. That was the worst one.

AL: Mine was very public when it happened. It was pretty secret, but as we pursued the bad guys it became public. I can speak freely about this one. Most CSOs of Fortune 500s can't discuss breaches in public. I can, and the reason is that we worked subsequent to the breach very closely with the Department of Justice and the U.S. FBI. It took us four years. We identified the perpetrators who had hacked my company and ex-filtrated some very sensitive data and supported the delivery of the first U.S. federal indictment against international actors for hacking an American company. The indictment is unsealed, so you can go on Google and read all about it. The vehicle was a phish, a simple email.

The email had an attachment in it. No subject, just an attachment. The attachment said agenda. That might not wake any of you up, except if I told you that the email appeared to come from a fellow named Carlos Ghosn, who has been in the news lately for other reasons. But at the time, Carlos Ghosn was a member at our board of directors, in addition to being in the leadership of Nissan. The email purported to have come from him to a collection of audience at Alcoa was from Carlos.Ghosn@yahoo.com. Nobody noticed the yahoo.com. They saw Carlos Ghosn the board of directors' member. They saw an attachment with the name agenda. They said, "Oh my God, I'm missing a meeting." Everyone who received it opened the attachment, which executed the initial malware, which is just the first step. Then that asset calls home like E.T., and says, "Send me more malware."

Then the bad guy uses all that malware to traverse laterally across your network and do lots of dastardly things until he has the most powerful privilege he can get. For example, Microsoft Exchange Administrator, Microsoft Domain Administrator, an Active Directory. Once he had that, he exfiltrated our entire credential bank – everything. And then used a now well-known tactic, Microsoft coined the phrase, "Pass-the-Hash." So you didn't have to decrypt anything. He used encrypted hashes of passwords, inserted them into arguments and was able to then log in as each of our executives and export their entire mailboxes. It wasn't a huge amount of data, if you counted the bits and bytes. But the damage, both to our secret operations, our intellectual property exposure, and even to my office, was significant. That was our major breach. Every company that has email, maybe even yours, has had the occasional minor breach. Everyone that's holding personally identifiable information has had an exposure at some point because by some definitions an exposure is if you have a collection of country identifiers, social security numbers, and you press the enter key and send it to one wrong recipient, inside or outside. If they weren't authorized to see it, by some laws that's an exposure.

I've had both ends of that end of that stick. I can tell you that first end of the stick is much more painful, when it's an intellectual property breach. But the personally identifiable information or personal health information breach is much more personally consternating because it affects human beings and not just companies.

BS: I was at Target during what was then one of the largest data breaches in history. To set the strategic context, it was the fourth quarter of 2013. Target was struggling with something you are probably familiar with and that was the Canadian expansion and the general failure of that business model. The board and the CEO were already under some significant pressure and then the FBI called and identified that there were millions of credit card records being sold in the Eastern European markets online where this kind of illicit transfer occurs. That was quickly traced back to Target. The identification of this breach didn't come from internal sources. It came from U.S. federal law enforcement who made that initial connection. By the way, that was on a Saturday morning when they picked up the phone and called Target's chief security officer, who was the former FBI assistant director.

The data breach in Target's case happened through a third-party vendor. There was a HVAC vendor in Pittsburgh. They had sold Target HVAC automation systems that did building automation. As a part of that, they had the ability to access Target's network through an encrypted private network VPN connection and because of mismanagement of the network in that it wasn't properly segmented, and some other basic security issues, they were able to fairly rapidly exploit that virtual private network connection and gain privileged access into the system. They installed malware on a number of POS systems in retail stores. First, to test that they could do it and then they rolled that patch out on their own across the organization into what wound up being most of the retail channel. What they were reading was the stream between the POS registers, which were just computers, to a server in the store and then out to POS, to the credit card processing systems. The stream had card holder data and they purloined about 41 million records over a period of several weeks. When this was discovered, it was still active across most of the organization. There is a Verizon After Action report that leaked to the press. You can find it on Brian Krebs's blog. He is one of the top information security writers out there.

They also gained access, Target revealed a few weeks later, to the guest data warehouse, which is 7 terabytes of data about shopping behaviour: an individual's demographics, what they purchased, how they purchased, what the company thought from a business intelligence perspective that this individual would buy – what you would promote to them. There was a ton of personal information that leaked out. I don't know that the guest data warehouse information is that valuable to anyone other than another retailer, but certainly 41 million card records will get you somewhere for a while until that gets shut down. Ultimately, this cost Target hundreds of millions of dollars, a portion of which was covered by insurance, a portion of which was not. The CEO resigned six months after the breach. Prior to that, a number of executives left: the CIO, the CSO, several officers within the IT organization.

RR: Alan, when we had spoken earlier on, you said the hackers that had breached Alcoa were after a specific type of data. Can you elaborate on the different types of data that hackers will go after and what we should be aware of?

AL: There are three general types of data. The first is the one that we read about most often, in terms of breaches that are publicized, and that's Personally Identifiable Information (PII). That has different definitions in different places. In the United States, PII is any two or more pieces of information that could be put together that could identify a unique individual. Typically that requires a social security number, an address, a name, and some other things. In Europe, by some definitions at the Union level, out of Belgium, PII is someone's work email address. Did you hear what I said? I didn't say their personal email address. Their work email address is PII. All of that is in that first clump that we call PII.

The second clump is Personal Health Information (PHI), which is obviously much more significant in terms of impact if it gets exposed. I had some early experience with a PHI breach before I came to Alcoa, many years before we worried about this kind of thing. I was running security for the University of Pittsburgh Medical Center, a large 16 hospital medical center. We had a very special patient. I can talk about this one too because it was all publicized at the time. Country Western singer Tammy Wynette was in the Medical Center for a liver transplant. There was a radiological technician who discov-

ered that she had been admitted under a pseudonym and if he could grab details about her and her treatment that he could sell it on the market. He sold it to the National Inquirer for $100,000 and this is 30 years ago. That's a boatload of cash. PHI falls into its own special category, at least for me, because of that event and some subsequent events. If you look at the U.S. federal law, there isn't any federal law about the breach or protection of PII. There is a law protecting and controlling management of PHI. We call it the Health Insurance Portability and Accountability Act (HIPAA).

RR: Over two years ago, a statistic found that over half the data breaches are incurred through third-party vendors or associates. Bryan, having had experience in that, what are companies – now that they are aware of that – doing to protect themselves from this sort of breach with their vendors?

BS: I think that third party risk is … there is an all-encompassing challenge around this and it's not just information security or cybersecurity. I think that a lot of companies have come to rely on a number of different service providers, particularly if you think about business process outsourcing and how a lot of companies use that idea of labour arbitrage in order to do their business processes. There are a lot of challenges around the resiliency, and security, and the ethics followed by organizations that you are doing business with. Having a good third-party risk program in place is critical. I think you have to look at all of those things holistically.

I think the challenge with the Target case is there were really two things at play here. The HVAC vendor probably never bubbled up on anyone's idea of a service that needed to go through extensive vetting because they were just a small service provider and you tend to focus on: Who are your biggest suppliers? Who are the ones most critical to your business operations? Second, there was an underlying challenge that even if they were able to penetrate the HVAC vendor (in Target's case), they shouldn't have been able to gain the privileged access to the network that they did. The VPN connection? Sure, to let them look at the temperature and the performance and such in stores, but they should never have been able to reach the POS servers and the point of sale registers. There was an underlying failure around access, that the network is properly segmented, and that you're vetting these critical vendors.

AL: Supply chain security, securing all of those suppliers and customers that are part of your ecosystem, that's an incredible job by itself. Even if you have secured your own shop to the best of your ability to mitigate as much risk as you might be aware of or concerned about. You can't reach your tentacles into other companies and impose an onerous set of standards that they would be required to adhere to in order to supply to you or be customers of yours. I think we'd all take the customer regardless of their condition. One last thing, French Philosopher Jean-Paul Satre had a definition of hell. He said, "Hell is other people." For me, as accountable to cybersecurity for a global organization, my hell was third parties. Because at least with my own organization, I knew my own exploitable vulnerabilities, I knew my weaknesses, I knew the Achilles' heel. I might not be happy about it. It might take a while to fix it, but I knew it existed. With third parties, it was almost a daily event that I would have a surprise, where I would learn that someone wasn't as secure as they should be, someone was not following the standard we at least recommended they follow. Invariably, that kind of concern rolled downhill. We were the largest single supplier for Boeing and the largest single supplier for Lockheed Martin, the largest single supplier for Boeing and the largest single supplier for Aerbus, for all the time that I was CSO. I can tell you that they saw me and my operations as Satre's hell.

JM: As we've moved into a digital enterprise, it's about the data. I think in our personal lives and in our business lives, we have taken that data for granted. If you look at what's happened with Facebook, with Google, with all of the apps, they add value to our lives. But they take something away too. As individuals, we haven't fully discerned our responsibility for protecting our own data and for recognizing what freely giving away our data means.

I have six grandkids and I never, ever post a picture of any of them. Because the last thing I want is for somebody to walk up to their school and say, "I know your grandma. See? I have her picture right here." We have to think about those things. And then in our professional lives, it's the same thing. That data that we take care of for our clients… in the health business one of my clients is Maryland Health Information Exchange. Everybody that goes to a doctor or Hospital in Maryland, D.C., West Virginia, their records go through our exchange. We hold their lives in our hands and we have to

take that responsibility seriously as we look at their data. That means that if we let it go, if we have a third party that we work with that does something with that data, we don't get to lose accountability for it. We have to know that that's still data that we are protecting. I am a real hard ass when it comes to the third-party stuff: These are our controls that we have in place. You need to show us that you have those controls in place too and if you deal with somebody else, you need to go check on them. We have to follow that chain because at any one point, they could bring us down. And they could lose data that I have sworn to protect. I think we have to take that personally and recognize that the data is our clients and that that's what the world is today.

RR: Do any of you have any comments on the Equifax breach?

JM: My view on that one is that we need a GDPR in this country, because we need to be able to have control over that. There are a lot of issues about whether Equifax was doing bad things. There is no exact standard of care, so I don't think any of us can in retrospect say, "Look at all the bad things they did," or "Look at all the things they did wrong." But if we don't have a way of looking at the data for what it represents and recognizing that we all have a responsibility to protect it, then as a society we've failed. The problem there is that we give our data to the credit card companies. They give it to Equifax. That's what's not acceptable. We've got to follow that chain and hold everybody accountable because we have no choice over whether they have our data.

AL: I lost my personal data twice within a year, both times when the same entity was breached, the Office of Personnel Management. I have a certain level of clearance in order to work with the FBI or the Department of Online Security, the DOD. In order to get cleared, I provided information I could not remember today if I wanted to, but the hackers know it all. And they didn't take it once. They had to be sure they got it, so they took it twice. At the end of the day, I do agree with the premise that it's all about the data but that doesn't get us closer to a solution. Let me give an example. In our case, we had these massive customers, the Lockheeds, the Boeings, who said to us, "If you want to do business with us, you are going to have to adhere to our standard." They gave us their standards and the standards conflicted with one another. One was modeled on ISO 27000; another was modeled on NIST 53 and 171, the U.S. commerce department service standards.

There was no reconciling the issue, which would have been: I would have been running separate security programs for each customer. And then, as an additional ask, they requested that we do very special things with data that we might hold for them. For example, lock it up in the equivalent of Al Gore's lockbox, if you remember him talking about social security years ago. If we locked it up, it would be very secure. The only problem is nobody would be able to make a part using that data, because it would be locked up and nobody would have access to it. Our customers didn't quite understand that premise. As of last year our largest customers were writing contracts that included clauses that not only said we would be accountable if there were a breach of their intellectual property, but that they would require us to meet a certain standard and they were attaching an addendum to the contract of about 110 pages worth of their cybersecurity standards that we were going to have to meet if we wanted to retain the commercial... Is that an answer? I can tell you that for us it was a bridge too far for us and our commercial people, and we decided that we simply couldn't cooperate.

JM: In my experience, that's not the typical situation. In my experience with IBM, with colleagues, that's not totally typical. There are a finite number of technical controls in security and privacy that you can put on things. The different standards can be confusing. The crosswalks comparing one standard to the other can make you crazy to find out if you've really covered them all. But they're all addressing basically ... the intersection of controls is pretty large. So if you get to that intersection, yes there are some one-offs, but the focus on those standards – and I think even more than that on the management system that addresses those standards on a very daily basis – can give you a lot of protection. Nothing is going to be perfect, but I think for data there are a number of controls that you can put around your data. You could focus a lot on access, on identity, making sure that nobody has access that shouldn't, and that you have different levels of controls there. There are elements that you can put on to focus in on the data to make sure that you are controlling the access to it. Not in a lockbox, but in a reasonable way so that people can work. Security's answer should never be: "You can't do that," but: "Do it this way." There is almost always a way to figure out how to get passed that. It sounds

like you were dealing with some very difficult… they sound like IBM lawyers.

AL: They were the only ones we weren't dealing with.

JM: But they sound like them; they're from the same cloth. But mostly you can get through that. You can't give up and you can't say: "We can't follow any standard because we can't follow all standards." You kind of have to follow one set that applies best to you. Maybe it depends on what industry you're in. The HIPAA guidelines are very stringent of … the good news is they are also very prescriptive. So if you get on board to following that standard, and you're in that space, you kind of need to know what you need to do to follow through. I have a better view of it. And in dealing with third parties, you could be very clear about which of the controls that are the most important and make sure that the third parties you deal with adhere to the ones that you think are critical.

AL: I agree with your perspective. What I'd add is that all of the controls that we might apply to protect our data in all of its guises (the PII, the PHI, the IP), all of it is going to rely on certain switches. For example: confirm who you are; authenticate properly; make sure that you're authorized properly. The difference being that authentication is who you are; authorization is what you can do. If someone at the same time is working in a background to steal your identity then the next time that he connects, he is you. And he will have all of the authentication and authorization that you have. I understand the premises for risk mitigation that have to do with making sure that only the right people have access to data. I also understand and your IBM example was a great one – making sure that you closed all of the exploitable vulnerabilities that you can that are almost new every single day.

Anybody use Facetime? So you know what happened yesterday, right? It seems that Apple is not invulnerable. Let's just say that. Almost everything that we do to protect data makes one key assumption, that there is somebody out there who is not authenticated properly, who is not authorized, who wants in. If you look at the kinds of data that you manage or work with every day, doesn't that data fall in that category? It is certainly valuable to you; it would be valuable to some adversary for some purpose.

JM: But hang on, because if you use multi factor than even if I were to use your identity, I couldn't necessarily be you. Multi factor is who you are, something you have, and something you know. All of us use it every day, whether we call it that or not because we probably use it with our banks. You get an authorization code to your phone. It's not impossible. There has been at least one example of the underlying communications network being compromised, but it is a very strong control.

We had a case with one of my clients last week through phishing. Identity was stolen. They thought the email came from a trusted source. They asked for the login information and one of the people who dealt with this person all the time gave it. I think that one went to somewhere in Africa. Very quickly using that account, they tried to come in. They couldn't get passed the multi factor. So they knew the person's ID, they knew the person's password, they couldn't answer… you can't get it until you use the code that was sent to your phone by text. They couldn't get passed that part, so they still got blocked there. If they hadn't gotten blocked there, our perimeters defences would have said: "Why is this person calling in from somewhere that isn't here?"

There are things that you can put around it. None of these things are perfect, but there are very strong controls that we can put around things. Mostly, you want to make it harder for them to get into you than it is to get into your neighbour. Because most of these guys… except for Alcoa, where they really wanted you, but in most cases what they want is to get in the easiest, fastest, cheapest way they can and then get out. In some cases where it is directed, that is a horse of another colour to deal with.

RR: As we are speaking with management of companies that we are looking at for the first time, what do we ask management around these issues, around what they are doing, about their data, their third parties? What are some questions?

AL: I'd start by asking them whether they have an organization that's focused on risk management at the enterprise level. Cybersecurity risk management is one part of an organization's risk management program. There's probably risk management for financials; there's risk management for environmentals; there's risk management for personnel

safety. For all of these things (one of them is cybersecurity), I would ask them if they have a risk management team and if part of that team is focused on managing risk for cybersecurity. I say "managing" because at the end of the day, we are mitigating risk. We are not eliminating risk. Nobody is going to make anyone in this room invulnerable – not by this talk, or by going to school, or by any technology combined. I know that scares you, but you're not invulnerable walking down the street either. This is the reality of the world we live in. Second, if they have a program of any kind, I would ask them what standard they do follow. At Alcoa, we would ask whether they were following the National Institute of Standards and Technology program, the NIST cybersecurity program.

RR: Is that the gold standard?

AL: No, it's equivalent to ISO 27000. Neither one of those standards (whether it's ISO or NIST) is 100% enforceable, 100% deployable, 100% useful. There is no one I know in cybersecurity who is deployed all of ISO 27000 or NIST 53171 – nobody. The scary part is, what people tell you in the marketplace (third parties especially) is "I'm good. I've got that NIST thing going. I've got this ISO thing going." What they are telling you is a lie. What they are telling you is they're working towards being a better cyber citizen, but nobody has yet achieved the gold star or the black belt for ISO or for NIST. The last thing I would ask, and I think you should always ask this of third parties, is that they be honest with you about any potential condition they currently have that might result in a breach and that they be equally honest with you about anything that has not been publicized in the past that was a breach. It doesn't hurt to ask. Sometimes they won't answer, but I certainly think it's worth asking.

RR: What are some of the red flags that we would see straight out, whether it's through a CSO's answer or lack of?

BS: I think Alan hit on a number of key things that I would want to know about. A couple red flags that would stand out would be if they've had breaches recently, or significant incidents, and they haven't mitigated or haven't really taken a good hard look from an after-action standpoint on what happened and be able to go back and correct those things. I would also look at: if they have such an organization as Alan described, where do they report? Are they part of the C-Suite or are they reporting to a C-Suite executive? Depending on the organization, either of those might be the right answer. I'm sure everyone has experienced this. I have a client whose CSO reports to the head of facilities; he reports to the head of shared services; he reports to the COO. That's not an effective security organization. By the way, that's a bank. Those are the kinds of things you want to look at. If I see a buried information security or an enterprise risk organization, or whatever it's called in that particular company, I would be very concerned about that from a red flag standpoint.

JM: I agree. I want to know if they have a program that they're managing every day. It fits in with this organizational thought that you've got to be placed correctly, but you've also got to have a focus. The controls we've been talking about fit inside what we call an Information Security Management System (ISMS). They can be built on any one of these standards. One, it's good to have one. And then manage it every day, which means you plan for it. You have policies in place. Do they have policies? You'd be amazed by some of the big organizations that haven't gotten that far yet. Are there policies and do they live their policies or are they shelfware? They have to have policies. They have to have processes that match those. These are the policies, the "thou shalts," and the processes are how you do it.

They have to have the technical controls in place. They need to measure them regularly. You want that internal organization to do its own measurement, because that's how they are going to continually upgrade and improve that program. And they need to be focused every day. They also need to be externally audited. I think that's absolutely key. They don't have to be perfect in their audit. Nobody will ever be perfect in any audit. That's what auditors do. They find holes. But they have to know where their weaknesses are. They need somebody other than themselves to say: "This one is really important, and you should be fixing it." So you should ask for audit reports, because they will help you know where the organization needs to continue to grow.

All of this has to be maturity based. There is very well funded, well disciplined, and determined adversarial community. If we fail to recognize that, we will fail to pay attention to this every day, and then we will fail to keep the bad guys down. Then the bad guys are selling their exploits. The bad guys

are very well funded. They come up with exploits; they use them; they sell them downstream. Now you have people who aren't so well funded, who can use those same exploits in new ways. So it's a very bad environment. What you need is for your organization to be constantly upgrading, constantly changing, and your audits will tell you whether or not you're going through that maturity process of evaluating yourselves, reacting to it, and modifying your positions because of that. Having that active program with somebody who is running it in a good position, structured into the organization, that can go into the top of the business and say, "This is a huge business risk," and have it make sense.

It wasn't a breach because nothing happened but one of the biggest risks I had to deal with at IBM was our competitive control systems. Industrial control systems are notorious for having problems from a security perspective, transportation… IBM's chip manufacturing plant was run by industrial control systems that were connected to the internet (because that's how they downloaded the material they needed from their vendors) and they were built on environments that were dependent on Windows XP, at a time that Windows XP had already gone out of service, which meant it was no longer getting security updates, and people were selling exploits to it all the time. If those lines went down for a day, it would cost IBM $3 billion. So I had to go into a group of our senior vice presidents and say, "This has to be fixed right now." Because as I was dealing with just the organization that ran the plant, they said: "We can't do that. It's too expensive to fix that." And that had to go up to the top of the business to say, "This is not a risk to that part of the business. It's a risk to IBM." In the risk framework, if you looked at it as a risk, that was a huge risk to IBM to not be able to produce chips. You need the organization to be placed at a point where they can go in and have those discussions. We got it fixed. I can talk about it now. They got it fixed. But you have to know that that person has that much capability to have those discussions.

AL: The one thing I'd add is that if you're going to have that conversation with a third party of any kind, you want to try and have that conversation on an equal or level footing. For example, if you're a bunch of financial people and one of you have been selected to have a highly technical conversation with the cybersecurity chief of this other company, then that's probably not equal footing. Instead, you probably want to have somebody on your team who's equally proficient technically, who understands risk, who understands the vulnerabilities throughout the world that we live in, and that can have that one to one conversation. Two things will happen: one, you'll probably get more honest answers because nobody would be able to funny it up. But also, because you will be presenting someone representing you, who has equal stature for the person that they are talking to, company to company, the conversation can get more real.

The last thing I'd mention, this is a follow-up to what you've said. I've said this before in other venues, and I truly believe it. We will never be more secure than we are today, cyber-wise. That means that every day going forward, we are going to be less secure. The reason I say that is because if somebody has … they need four qualities. If somebody has the time, if somebody has the money, if somebody has the skill, and if somebody has the inclination to hurt you, will your organization always have the time, the money, the skill, and the inclination to keep it from happening? I can tell you from my experience that the answer is no. That means that the bad guys will win more than they lose and by equation that means we will (as the good guys) always lose a little bit more than we win. I know it's scary.

RR: Is there a way we can have that discussion at a financial level? From a resource perspective, just by asking some of the companies how much they invest in cybersecurity and how they allocate that investment? Will that help us understand high, medium, low, what the risks are?

AL: There are at least some basic guidelines. Gartner, for example, they are a research company and they do a lot of IT research. They would say your cybersecurity budget should be 6-8% of your annual expense budget for IT. In my case, it was actually almost exact. Our annual IT expense budget, operating budget, was about $312 million, and my budget was $24 million expense. It was just about that 8%. I hear people in the community, in the cybersecurity space, talking about 10%, 12% of IT spend. At some point, we will believe that the tail can actually wag the dog, and that will not happen. Somebody will stifle it. Somebody will say, "You know, we can only afford to be so secure. And then the money will… if it won't dry up, it certainly won't increase at the rate it has been.

JM: I think you can throw too much money at it too. That's

another risk. If you can place it securely in a risk framework, that's more important than how much you spend – how it's viewed, how it's managed, where in the business the risks are considered. Because truly spending too much, closing too much down, there are things you can do in security that will make you less secure if you do them wrong. It's a good benchmark, I agree. Gartner will tell you that, but Gartner gets paid by a lot of people who sell products and want to push it out there. Maybe it's a good starting point and if they are way under that number, they probably aren't paying attention to it. But trying to get to where they focus on it, how they focus on it, how they consider it – from my perspective, is also a good approach.

BS: I think the programmatic aspects are going to outweigh what they are and are not spending, but looking at the financial spend for cybersecurity can give you some context that might point you in the right direction of questions to ask.

AL: And ask about the size of the team, the location or locations of the team, what skills they expect from the members of the team. There are non-financial questions you can ask as well.

RR: Are there companies out there that are doing cybersecurity really well that we can follow?

BS: It's going to be companies that you're typically not seeing. That's the danger of this question, it's the companies that you're not hearing about that are either lucky or good or have some combination of the two. I don't know if I can name a specific company that's necessarily doing it well, but look in the spaces that you're looking to invest and see who is not in the news for cybersecurity issues.

JM: The one thing that no CSO will ever do is say how well they're doing. That just puts an enormous target on your back that you don't want, so it's not something that people brag about. But I think you're right. If they're not in the news, then if they are getting hit they are managing it really well so that it's not becoming a public exposure or they are getting it before it gets really bad for them.

AL: The FBI report, the statistics are pretty standard year on year. The U.S. FBI says the bad guy will be inside your network for about 264 days before you know it. That company you admire because they have not been hacked may actually be in the process of being hacked and they don't know it and that's why you don't know it.

I'll give two examples of companies that I admire for their programs. One would be Lockheed Martin. There is a good reason for that. They do a lot of defence work and the DOD in the U.S. essentially gives them a blank cheque. The other side of it is that I admire J.P. Morgan for the amount of money they spend on cybersecurity. That number is half a billion a year; however, you'll be aware that within the last 3.5 years J.P. Morgan had a significant breach. The numbers didn't go up dramatically after that. They already had a significant spend in cybersecurity. The lesson there is that money alone is not the answer. Two little will hurt; too much won't help.

RR: You talked about companies doing a good job of keeping themselves out of the press, but I also wonder if you have a sense of instances where hackers are able to come in and then close everything up and nobody knows they were even there? Is that pervasive across businesses?

JM: I guess the secret there is that we don't know. Could there be that? Absolutely. There was a great study done on a mid-sized company of large equipment. The hackers were in and in for a very long time undetected and were able to destroy the supply chain. Orders didn't come in well; equipment didn't go out. This was a very well-managed company previously. They couldn't figure out why things were going bad. Later the finances started getting messed up and they couldn't figure that out either. They ended up selling out. This was a foreign national company that came after them, implanted that in, did the exploit, and the ones that exploited them was the company that bought them for 10 cents on a dollar. And it was known only after they were bought out and lost everything that this deep analysis was done to figure out what had actually happened and it was understood. Yes, those incidents are out there. There is no way... this one, things were going bad and they couldn't figure it out and they had been well managed. Maybe it would have been good for them to stop and say: "Something is going on that's in the systems." And they didn't, because they didn't know to be aware of the cyber issues. But that was very much a retrospective thing.

RR: What are your thoughts around cybersecurity insurance? Is it worth it?

AL: That's what I'm speaking on… I have two panels tomorrow in Manhattan. Cybersecurity insurance has been around for a while. It's getting more interesting, meaning there are more offerings, more variations in terms of what the insurers will cover. The deductibles are still being processed. The premiums are still being processed. By that I mean, nobody really knows what they should be charging for this stuff and some insurance companies have already taken significant hits by undercharging. Others are making out because they've been overcharging all along.

It's very difficult because: how does an insurance company value risk? They do it over time, by precedent, by history. There isn't enough history here in terms of quantifiable damage. There is for a Target. It's a public company, so you know how much in their 10-K or their quarterly SEC filings how much they needed to spend to remediate the problem. What will never be covered, and this goes to the heart of one of those three categories of data I talked about earlier, what will never be covered is IP. Because every insurer will tell you that intellectual property can't be insured until it can be valued. And it can't be valued until it's exercised in the marketplace. Meaning that you've actually used that IP to produce a product and then that product has gone on for sale.

Of course, if someone is stealing your Coca-Cola recipe, they are going to be marketing it before you are. So they'll never be a way to value what you've lost. So the insurers aren't doing that. They do the standard stuff. The business continuity, disaster recovery stuff, they've been doing that for years. They are all now, almost all, the big ones – For example, Chubb, which is the largest in this space – are doing a fair amount of focus on PII and PHI breaches and how they can keep an insurer whole. But even there, what do they offering? They are going to offer a certain amount for damage control, a certain amount for public relations, identity theft protection for one year, for each person who's been harmed, and not a lot else. So you can insure for that. Alcoa at the time was actually self-insured and as it turns, based upon our own analysis, it probably wouldn't have made a difference because it was intellectual property, which couldn't be insured anyways by a carrier.

JM: Business interruption insurance is also challenging, based on cyber incidents. If you have a lot of personal data and you're going to have to go out and pay people, you really want it because that's where it's going to protect you the most. But you have to be careful. And I agree. There is just not enough actual real data out there to make them smart. On the other hand, if you have personal data where exposure could mean lots of money to take care of people for a year, you want insurance for that.

BS: Target had cyber insurance as part of an overall risk management insurance strategy. The company was self-insured under $20 million in loss for pretty much anything. This was obviously way above that. I think the broader cyber insurance question is that it has to be part of what the company looks at just in terms of their whole insurance package. What are the right things to put in place in order to protect themselves? I think Joanne is exactly right that if the company has a lot of personal information (as Target did in terms of cardholder info), it's probably a smart move to have something like that because just the management of notifications of the breach and the credit monitoring and the process that you're not necessarily required by law to do, but you want to do because it's the right thing to regain your reputation in the marketplace. Certainly notifications, there are some legal requirements by state in the U.S. anyway around that.

AL: I know some brokers, I know their programs intimately, who are selling cyber insurance as a replacement for some portion or portions of the cybersecurity stack (that thing we all call defense in depth). You don't need to do that from now on, you can just get insurance instead – that is obviously a big mistake and a huge fallacy. It's an addition to the stack. It's a supplement to it. It doesn't replace anything in terms of technology, people or processes that an organization is doing to be cyber secure. The last thing I'll mention on security is that it kind of is an ironic situation: cyber insurance for cybersecurity. Because what is cybersecurity but an insurance policy itself? It's a term-like policy not an ROI, so it's not whole-like or universal. It might build a little bit year-on-year, but name a company that is doing cybersecurity because they want to as opposed to because they have to. What are you insuring against? Life insurance, a term-life policy – you're betting you're going to die. Cybersecurity, all of your spend – you're betting you are going to get hacked. You're betting you will be a target. In that sense, cyber

insurance is cyber insurance for cybersecurity, which is by itself insurance.

RR: Each of you have touched on what I think are the key components of the cyber programs. We talked about controls, vendor management and alignment with international standards. But how do you measure, in your experience at your various companies, how to effectively create a security-conscious organization where everybody at the company thinks about it and the behaviours are there. You're thinking about everything you do, every decision you make in a security-conscious way. How do you build that and maintain it? How do you look for it when assessing companies?

JM: Our biggest threat everywhere is our people. It's always going to be the person who tried to do the right thing because they got an email from the CEO that wasn't from the CEO. It has to be from the top down. The CEO has to believe that this is critical, that the culture be security minded. The best case I saw of it when dealing with different companies was Shell oil, which has a very strong security program. If people didn't follow their security guidelines on the platforms, people died. So they took their safety very seriously. They talked about it from the top down. They talked about it at executive meetings; they talked about it all the way through the organization. They would open meetings with it and say safety matters.

When they went in to focusing on cyber, they did the same thing. From the top of the business down they said that this is a core, cultural requirement and not our lives, but our business depends on it. They trained on it, and they trained again on it, and they talked about it every day. They had posters. They did everything that said: The CEO cares. Your business unit cares. This matters to keeping us going. You really need that level of involvement. Fortunately at this point, there are lots of good training programs. There are lots of good phishing exercises that you can put out on a really regular basis, so that people get scared every time they see an email. But that's what you want. It has to be from the top down. You want people to be sending things asking, "Is this phishing?" because then they are thinking about it. There are lots of programs that do that. They aren't that expensive; they are really critical to use, but from a cultural perspective if the CEO doesn't buy in, doesn't take the training individually and doesn't champion it, you will lose the culture battle. It has to be throughout the organization.

BS: I definitely agree that it's got to come from the top. My own Target experience is that I had a CEO who was interested in compliance because, "Well, I've got to comply with PCI and I have to comply with HIPAA, and I've got to do this and that's all I'm willing to commit to on security." Well, the determined adversary doesn't care about that. They don't care that you are PCI compliant. They are coming after your program because if that's all you're doing, then it's going to be relatively easy for them to go to the next level and figure out how to get into your system. I also like to see evidence that they are doing some of these things. One simple thing I like to look at (this is more on the response end): Are they practicing their response through effective exercises, through a cybersecurity incident, or pick your crisis – reputational crisis, natural disaster, whatever it is – and are the senior executives participating in these crisis exercises, cybersecurity exercises? Or are they just letting the middle management drive the answer to that? If they are not participating and they're not involved in that, then I would question if there is really the executive commitment that you're looking for in that organization.

Audience Member: Can you share some examples from your personal life habits where you're protecting your security or your cybersecurity?

JM: I have a personal VPN that I use for when I go online. You can buy one. I have a passwords safe. My passwords stay in there so I can have complex passwords at different sites that I don't have to remember because I'm old enough that that's hard. I try to be aware. I don't have Alexa, I don't use Siri, there are things where I just draw the line. I had a conniption when my daughter wanted to buy one of those baby monitors for the house. She has one anyways, but that's over my objections. I think, again, it's a matter of awareness. I think about what data I give. Whether I give it or not they probably know it, but I'm not going to surrender it myself. I'm very thoughtful about those things and I limit the places that I share information with. I try to be very mindful of that.

BS: I'm similar. My wife and I work together and we have young children. We are very careful of what we post online. We built a home six years ago and we took a number of measures to

conceal the location of our residence from easy ways to get a hold of things, for privacy purposes. But social media is probably the biggest area. We are very careful about how we distribute pictures of our children and talk about where they go to school, what activities they're involved in. We keep that to a tight circle of family and friends on Facebook, and we don't post any of that anywhere else that's more publically known. I'm probably more paranoid than most, but our home security and network configuration has very little Wi-Fi, lots of hardwires so it can't be accessed from the outside. Twenty-one years in corporate security will make you do some strange things.

AL: I've been victimized on a personal level, but it was a result of what I was doing on a professional level. . I had a Gmail account that was hacked. I had a Yahoo account that was hacked. Every one of my bank accounts was hacked. I have two daughters who had university accounts and Gmail accounts. They were all hacked. My daughters' bank accounts were hacked. Until, and maybe this is a lesson for all of us, I came up with a moniker that could not be associated with me in any way. I'm "ice cream truck man" on the internet. That's as opposed to cybersecurity guru, right? – Ice cream truck man. I chose to have my mailbox on AOL for good reason. There is this notion of security by obscurity. But I think that in this day in age, to say to people generically, "Just withdraw from social media and you'll be safe." That's not a good answer. That's like withdrawing from oxygen at this point, so there have to be better answers. I'd recommend AOL.

JM: Constant vigilance too. I talked about having people be very nervous because of all the testing we do for phishing. You want that nervousness. I got an email from the FBI because they wanted to know if we wanted to have a connection with one of my companies that I was working with. Before I responded to it, I went online and looked up the local FBI office (not that individual, but the local FBI office). I called them and I asked for the name of the individual who would be doing this kind of outreach. Once I knew that and I said, "Is this the email?" They said, "Yes." I asked, "Would he be doing this type of research?" They said, "Yes." And then I answered it. That may sound obsessive, but you need to be that suspicious. The one at the client where one person clicked and gave credentials, I looked at it and said, "That looks funny." Because it was a business email that was just very unprofessional in my view. So again I went online and looked to find out who the individual was that was sending it. And then if you scrolled over, it was very clear that the thing they wanted you to click on wasn't the right address. Be mindful. Slow down and be mindful, especially at busy times of the year. If you have busy times of the year, that's when you're going to get hit. So be very mindful and take all those precautions because the time that you don't is the time that it will be hurtful.

BS: When traveling to what I would consider a high-risk country, leave your stuff at home. No electronic devices. Rent a smartphone. Don't do email; don't text. Do the absolute minimum. Leave the laptop at home. If you have to take a laptop, take a clean one. When you come back, wipe it.

AL: The last thing I'd add on that topic is that social media has not really been our friend in all of this. Think about the most popular social media. Let's just pick Facebook and Twitter. What's the login user name? In all cases, it's an email address. I have done ad hoc informal surveys of folks in rooms like this where I've turned around and said, "I don't want to know who you are, but tell me how many of you believe that because you are using an email address as your username that the password for that thing, let's say Facebook, has to be the password for that email address?" Typically, it's about a 30% return. Not in this room because of course you're all so smart, and we are in Canada. But in the states, to think that 30% of folks that I would just randomly survey in a room like this would believe that the password for their Facebook account must be the password for their email address because their username is their email address... There are simple things that you can do and there are probably simple things that social media might be able to do going forward to make life easier. Why they all decided that an email address was the perfect username is beyond me.

Audience Member: You mentioned that under the insurance if there is an issue that insurers will pay for identity management or identity theft protection services per year... what is your impression for the quality of those services and the value they offer?

AL: It varies. None of it is pristine and perfect. It's better than nothing. It is funny that you have people like Equifax who are offering identity theft protection. Do you see the irony of

that, or is it just me? But you have the LifeLocks of the world. Every one of these services is relying on other services to get input. Anybody who can fool you can fool your lenders, can fool all of the other folks you need to associate with in commerce and in life. So at the end of the day, garbage in and garbage out is what they've always said about computers. The ability of these entities, these services, to protect your identity is limited. There is a good reason why the LifeLocks of the world will offer up to $1 million of protection if your identity is stolen. It's because you'll never be able to prove it, and they'll never have to pay up. By the way, to this day they never have paid up once.

JM: On the other hand, I do have all of my credit locked with all three agencies. Maybe it's different in Canada. I don't know. But if you go through companies like Equifax, all of my credit is locked down so that nobody can check it until I open it and I say, "Okay, this company can check it." I had to get a mortgage, and I had to go in and at all three services I had to say, "Open it to this organization for 24 hours and then lock it again." That's just one more protection you can take for yourself.

Audience Member: At the enterprise level, you would use vendors for network securities, firewalls, end-point securities, things like that. How do you go about evaluating those credible vendors that you want to actually bring in vs. the ones that are just offering snake oil?

JM: Product vendors or services vendors?

Audience Member: I'm talking about someone like a Symantec or a Palo Alto Networks or a Trend Micro?

AL: More like services, right? Where they are supporting your internal programs? They're not just selling you a thing.

Audience Member: Maybe you could explain the difference.

JM: Products: you're going to buy a piece of software that you are going to put on your system that gives you anti-virus protection. Service: you're going to have somebody who monitors that, manages it, makes sure that all of your systems have it and that it's rolled out appropriately and all of the patching is maintained and you don't have to do that. Companies do both. Organizations do both. You vet them slightly differently but in both cases in security I would put reputation as the number-one factor. Then with specific requirements Gartner helps. Gartner has what they think are the best vendors. There are other places that do, but I would say that reputation in the industry is very significant. Just understanding what people who are using them say about them can tell you a lot. I work with a private equity firm that's looking at doing acquisitions in the security space and that's one of the first things we look at is how they are viewed. In their case they are looking at whether they need to be better managed, because then we can make some money on it. It's like flipping a house. But it also tells you something about how companies are responsible in their actions.

Audience Member: What would a good reputation vs. a bad reputation sound like?

AL: It's interesting you mention that because there are companies now that will actually score you, and score you so that you can keep it private and only hand it out to potential customers if they ask. And in some cases actually publish it publically. They will ask you to fill out surveys. They may do some penetration testing of your network. They may do a vulnerability assessment. Then they'll say, "You're an 8 out of 10." It's more detailed than that, but it's that kind of thing. The distinction I thought you were making earlier was: If you're not doing security yourself but you're having somebody else do it for you, what we call a Managed Security Service Provider (MSSP), whether they are holistic and doing your whole program for you (there are lots of folks who will take their money and do that) or whether they are just doing a part. (They are just managing your perimeter security; they are just managing your endpoints; maybe they are just managing your cloud relationships, or just your data.)

The problem with every one of these services, regardless of the reputation, is the same. When you're the CSO, as we've been. We've served these senior roles. You are responsible for security. Every day, what does your team do? It does security. When you sign up with an MSSP for any reason – and some of these are gangbusters, much better than you'll ever be at doing what they do – you're now no longer managing security. You're managing a service-level agreement with (in most cases) minimal visibility. They won't show you everything that's under the hood of how they do what they do. They may not let you know about every incident they see

because it may implicate weakness in their own program. You go from managing security to managing a legal agreement. There are sweet spots where that works. Where do you see the cut? Much larger organizations tend to discreetly select service providers where they believe there is a … that may support their program. Smaller companies tend to do the whole hog outsourcing (Come and run my whole program for me) because they can't find the talent, and they don't want to take the time to run a program themselves.

RR: If you were CSOs of a Burgundy, what would you be doing?

AL: Living in Canada would be number one.

BS: There are probably two areas of focus. (1) Protecting your organization; and then (2) how can you provide resources or expertise to the organizations that you're investing in (or, in some cases, perhaps to your clients as well)? Internally, we've talked a lot about what makes a good cybersecurity program. I don't know that I have anything new to add to that. But I know a number of firms in your space where part of what they do is provide services or provide expertise to their portfolio of investments to make sure that they have what they need to have. That they have what they need in place to adequately protect their intellectual property or data that they're holding. So I think that's another area to look: what expertise are you able to provide downstream to the companies you're investing in or in some cases, to your clients?

JM: I recently worked with an asset management firm and I fired them as a client. They started out saying what they wanted to do was build a security program and get themselves secure because they had so much client money (individual and institutional) that they were taking care of. They wanted to get secure. They wanted to do all the right things. But what became clear was that they wanted to be compliant and compliant is not secure. I think it's still true that everybody that's had a PCI type of breach was PCI compliant. Compliance is not the same as secure. To me, what you want is security. You want to get out ahead of things. You want to have that risk framework in mind that says: "I'm going to manage this all the time." Not: "I'm going to check boxes." Because if all you do is check boxes, you'll make your regulators happy for a while until you have a major problem.

Audience Member: Can you touch on the current regulatory environment and what your predictions are for where the regulators are going to go on cyber risk?

AL: Let me give you the short answer. The current regulatory environment is mixed depending on where you are in the world, and it will grow over time to consume everything that we're talking about. That will happen in Canada. It will happen in the United States. People point at things like the General Data Protection Regulation (GDPR) for the European Union and say, "That's the be all and end all of security." No, it's actually silent on the topic of security. I hope you've read the regulation. It is very articulate on the topic of the importance of protecting personal identities and personally related information. But it doesn't tell you how to do it. It tells you what's going to happen if you do it wrong. That's that 4% of annual revenue. But it's not the structure for having a cybersecurity data protection conversation. It's the enforcement if you don't have a program. In the United States, as you may know, California is taking the lead, as it does on lots of things because they are so West Coast. Well, so is Vancouver. It's pretty West Coast. They are taking the lead on what will be the first substantive legislation at the state level in the United States for the protection and defense of personal identifiable information. It will be silent on how to do it also. It will prescribe some direction. It will say: Why don't you look at ISO; why don't you look at NIST? Why don't you have a "good structured program?" And then you'll go elsewhere in order to get what you need.

The last thing I'll mention is if you looked at the way the federal government in the United States operates, you can tell who the folks who care about cybersecurity are and who are the folks that do not by the regulations that are being developed. For several years, the Defense department has had something called the Defense Federal Acquisition Regulation Supplement (DFARS). You can't do business with the DOD unless you meet a certain level of standard in terms of your cybersecurity program. If you look at DHS, which is in the news almost every day in the United States for a variety of reasons having to do mostly with Mexico, the fact is that there is no regulation on cybersecurity at the DHS level. And there is no privacy regulation at the federal level in the United States. What we do have is breach notification in all 50 states. If you realize that we've sent those social security numbers to the wrong recipient, here is what you do. You

know what you do in New Jersey? You call the state police and report it over the phone. That's how structured things are in the U.S. in terms of regulations right now – not very structured.

JM: I'm not sure that's bad. One of the challenges with regulations is that by the time they're in law, they're out of date because cyber moves and the threats change, and there is no one standard of care. The challenge is that for every industry, the threats are different and you need to be able to respond to the threats and the risks to your business, not to something that people put together as: this is the be all and end all. If you put it too much to the regulations, I think you miss that ability to respond quickly and you put yourself back into a compliance mode where you are answering yesterday's problem because that's what the compliance is addressing. I like the notion of the frameworks that NIST put together. I like all of us having some personal responsibility in terms of looking at those frameworks and saying: "This is what mattes here and this is why it meets my business's risk framework." If you look at smaller businesses especially, some of the regulations would be way too heavy for them. They need to be able to decide: "These guys manage risk every day. Smaller businesses are probably highly at risk of going out of business, so they are constantly managing a lot of risks. Cyber is one more. They need to be able to manage that. So we need good frameworks. We need good directions. We need good explanations and understanding.

For data privacy we need regulations because then you're talking about individual information and my right to tell you that you can't use it, as opposed to the other way. The other problem I have with the regulations and them coming down hard on people is let's be real. If I get breached, it's because somebody was a criminal. Let's go after them. Let's not go after me. I don't think we usually go after a bank that gets robbed and say, "You were bad." Maybe if they get robbed every day for a while then you would say that they are doing something wrong. But they're the victim. So the regulations tend to make the company who is trying to have a secure environment the bad guy instead of the victim. I think we have to take that into consideration too. I think there is a range of issues that jumping to regulation too quickly would be wrong. I know that's what happened with the NIST framework and why it was decided that that would be a framework and not a regulation, and I think I like that function.

BS: I think this is probably only tangentially related to regulation but at the federal level in the United States, the government can't even decide who is going to be responsible for cybersecurity. Alan mentioned the DOD. The U.S. Department of Defense has some standards out there. They also have United States Cyber Command, which is both a defensive and offensive military unit.. There is the National Security Agency (NSA), which is an Intel agency that sets some standards that are followed and – certainly from an encryption standpoint – has effectively led the way for decades around that. The U.S. Department of Homeland Security has been responsible for critical infrastructure protection, but nobody can really decide what that is. I've worked with them for 15 years trying to figure out where retail and retail banking at Target fit into all of the things that we are trying to do.

JM: And this is commerce.

BS: And this is the department of commerce. And we are probably missing a whole bunch of other agencies. There is a lot of disagreement about who takes the lead and who would do the regulation. So you definitely have a patchwork approach, at least in the United States.

AL: And then you have regulations that are popping up from the oddest places that want to impose a structure on cybersecurity. I'll give you one example here that impacted us in ways we couldn't have expected. It's called Chemical Facility Anti-Terrorism Standards (CFATS), U.S. statute. It's a regulation, and it says that if you're a facility that handles or has chemicals that could be used to make bombs that could be useful to terrorists, you need to have certain protocols in place to protect those chemicals. For the last four years, they've aided a cybersecurity regime to that program because, obviously, chemicals are transmitted by wire. I guess, nowadays I'm not sure how. My point is that from the oddest places, the worst thing will happen. The people who should have the least to say about what good cybersecurity should look like, will probably end up having the loudest voices because the voices we should hear from are remaining mum.

JM: To go back to your question about where things are going, I don't know on the cybersecurity perspective. I think on privacy, probably the right way. I think that's the one you probably care about the most because you have a lot of personal information that you have to protect. I believe

this country will move to something like GDPR because being responsible for identities, being responsible for personal information, being accountable to your users that you will forget them if they want to be forgotten, everywhere in the system they will be forgotten. That's different from protecting your environment. I think that's a place where regulation should and will come. I would hold privacy different from the security regulation because of the intent of it.

Audience Member: On the topic of privacy, a lot of companies that sell data say they anonymize it. Is that actually possible? Do these companies really protect anyone when they sell data, like Google or somebody, can they actually anonymize?

JM: Different question between if it's possible and if they actually do it. I believe it's possible.

AL: But still the source would have to be...

JM: There is somewhere where it can be brought back together.

Audience Member: How much of the targeting by hackers is industrial espionage, trying to drive down a competitor or infiltrating another country and their industry vs. trying to steal personal data so that you can use their identities to buy things and ship things?

BS: The perpetrator, the adversary at the other end of the equation, is different in most cases. In Target's case, it was an organized criminal group that was targeting Target or trying to find any retailer they could get into to take payment card information. I think when they are going after intellectual property, if it's not a competitor who happens to be really savvy from an information security standpoint then it's a nation state at the other end of the equation.. The end equation of who is at the other end of the wire I think is very different in those cases.

JM: I think it's true what I said before that some of those exploits are developed by the high end for those purposes but then sold to people who aren't experts in exploits at all and go after other targets very easily. I'm not sure how important it is to differentiate exact numbers so much as to know that there's this spectrum of possibilities and it could be any of the above.

AL: Certainly, the dollar value on PII breaches is pretty well documented year on year. It's in the billions, and it's growing every year. But to answer your question a different way, I think this rising tide of cyber risk is lifting all boats. By that I mean that it's not a see saw. As PII becomes less risky, IP doesn't become riskier. I think it's all of it. All of it is getting riskier. Different strokes for different folks, so there are nation states who are very interested in intellectual property, stealing it from countries like yours and countries like ours. There are lots of criminals who understand what we understood in America back in the 1950s, you want to rob a bank because that's where the money is. These folks have figured out how to do that digitally, whether it's with fraudulent or embezzling emails: "I have your grandchild. He needs an operation. Send $5,000 now." – You know the games. At the end of the day, all of that risk has gone up, to all kinds of data across the board. The more we share it, the more at risk it will be. I'll say one last thing that will probably frighten you all. The more we care about it. The more important that data is to us, the more important it will also be to some adversary some place.

JM: I have to be a bit of a Pollyanna because I think there are some good things too. As well funded and hardnosed as the adversarial community is, there is a really active community of people on the good side too. There are new techniques. There are new tools. I think there is a lot of value that's coming out of the machine-learning techniques that are being applied across many of the towers in security. I like the approaches of using behavioural analysis. If you usually come in and do these five things and today you do that one over there, maybe I want to know why. As we learn how to monitor better, that's all good. The other thing that's happening is these tools are gaining intelligence so that there is a limit on how many security experts we can have in the world, but as we add intelligence to the tools, they can offer up things to look at that aren't: look at everything, but look at this thing. I believe that kind of automation is going to help the problem too.

This is not all doom and gloom, and if you can approach it understanding your risks and knowing what you ought to be looking for, there is a lot of movement in the research and development community that is coming out with better ways to protect yourselves and to put defenses in place.

RR: That's a positive note to end on, a very big thank you from everyone in the audience for your time.

BURGUNDY
ASSET MANAGEMENT LTD.

TORONTO

Bay Wellington Tower, Brookfield Place
181 Bay Street, Suite 4510
PO Box 778, Toronto ON M5J 2T3

Main: (416) 869-3222
Toll Free: 1 (888) 480-1790
Fax: (416) 869-1700

info@burgundyasset.com
burgundyasset.com

MONTREAL

1501 McGill College Avenue
Suite 2090, Montreal QC H3A 3M8

Main: (514) 844-8091
Toll Free: 1 (877) 844-8091
Fax: (514) 844-7797