ASPEN INSURANCE

CYBER RISK AND THE EVOLUTION OF SUPPLY CHAINS

aspen-insurance.com

In collaboration with Columbia Business School
AT THE VERY CENTER OF BUSINESS™

CYBER RISK AND THE EVOLUTION OF SUPPLY CHAINS

Global supply chains are a way of life for modern businesses, but in the constant search for affordable labor and services, new challenges and risks have emerged. Businesses must contend with the added complexity of managing production across various locations in different parts of the world, and manage each location's individual risks, from political unrest to natural catastrophes. The 2011 Tōhoku, Japan earthquake and tsunami drove home the realization that a single point of failure at a single link can halt the flow of goods across the entire supply chain.

To meet the new challenges, businesses are finding new ways to increase communication and coordination across their supply chains, using technology to integrate systems. At the same time, they are creating redundancies in their supply chains, allowing them to divert production to an alternate location should a supplier be taken offline for any reason.

Amid these trends, cyber crime lurks with massive financial incentives for criminals and an increasingly connected world on which to launch attacks. Some supply chain trends play into the hands of those who perpetrate cyber attack. For example, efforts to integrate supply chains by connecting systems and getting them to talk to one another creates opportunities for cyber criminals to infiltrate systems throughout the chain by infiltrating the weakest link.

However, some of the tactics businesses are using to manage supply chain risks can also be used to manage cyber risk across the supply chain. Companies that make serious efforts to audit their supply chains to better understand risks can also assess their suppliers' and vendors' cyber security efforts. And the trend toward creating redundancy in supply chains can help businesses should a cyber attack take down a supplier.

This white paper will explore emerging trends in global supply chains and cyber risk, outlining strategies businesses can employ to protect themselves and keep the flow of goods and services moving in a world where cyber criminals are constantly adapting their own strategies for launching disruptive attacks.

THE EVOLUTION OF SUPPLY CHAINS

Supply chain development is proceeding along three dimensions:

- **Supply chains are becoming more global and complex** — The outsourcing era continues as companies identify new affordable places to produce their products.
- **Supply chains are becoming more integrated** — To fight increasing complexity, companies along supply chains are leveraging technology to collaborate and better coordinate their decisions.
- **Supply chain optimization** — Companies are trying to optimize their production, inventory, and logistical decisions along the chain, bringing the concepts of lean production and six sigma to supply chains.

Dr. Fangruo Chen, MUTB Professor of International Business at Columbia Business School's Decision, Risk, and Operations Division, explains, "If you think about supply chain evolution, or innovation, in past few decades, think of it in terms of the scope being more global and more complex, the relationship between members of the supply chain becoming more integrated or more cooperative, and, finally, companies improving the quality of decisions through optimization and identifying technology solutions and strategies that help them effectively manage and make decisions across the supply chain."

SUPPLY CHAINS RISKS

The evolution of supply chain development has brought with it an evolution of risks. Because supply chains have become so extended, a problem at any link in the chain can cause major disruption for multiple parties. Essentially, a failure at a single point in the supply chain can cause a bottleneck that slows or halts the flow of goods. Potential risks coming from many directions. Natural catastrophes can disrupt suppliers and cause capacity issues, notably seen in the aftermath of 2011's Tōhoku, Japan earthquake and tsunami [1], and, more recently, when earthquakes struck the south of Japan [2] in April 2016.

This risk is not limited to the physical production of a good: a company may be dependent on a vendor for payroll, security services, or benefits. An outage at any of these suppliers could cause a significant knock-on impact for the company relying on the service.

Other risks abound. Political risk around the globe could halt the flow of goods along a supply chain, as could the failure of a machine at a supplier's factory. Beyond the flow of goods, the quality of products can be compromised at any point along a supply chain, from the raw materials to the semi-finished product. A recent, prominent example is the massive recall [3] of all Takata-made ammonium nitrate-based driver and passenger airbags that do not using a drying agent, affecting a wide range of car makes and models across a number of model years.

The complexity of supply chains has also changed the liability landscape. A company may be ultimately liable for quality issues that occurred at a supplier. "This is a changing environment, and it seems like it's more and more true that companies will be responsible for what their supply chain is delivering," Dr. Chen says. "It's not just what you do, but what your upstream suppliers do." Dr. Chen also points to "invisible risks" in supply chains that companies have to anticipate, which gets complicated when real money has to be spent to try to prevent them. "Potential is hard to quantify," Dr. Chen summarizes.

> "It's not just what you do, but what your upstream suppliers do."
> **Dr. Fangruo Chen,** Professor of International Business at Columbia Business Schools

COMBATING SUPPLY CHAIN RISKS

Companies have adapted to the changing environment through supply chain risk management — where risks to the supply chain are constantly assessed and strategies are developed to manage them. Steps include:

- **Audit programs** — Companies are making a continuous effort to get more information about what is going on along their supply chains, and they are taking proactive steps before disruptions occur. This includes company executives visiting and inspecting production sites, with Apple CEO Tim Cook visiting Foxconn's manufacturing plant [4] in China being one well-known example.
- **New supply chain design** — Companies are looking at making supply chains more robust and able to deal with global risks. For example, diverting production should a problem occur at one link in the chain. As Dr. Chen notes, this is "easy to say, but very hard to do."

WHERE CYBER RISK FITS IN

It's hard to avoid the topic of cyber risk today. It is a threat to businesses of all kinds, even in sectors far removed from retail, banking, and healthcare, where breaches have been well publicized.

Attacks come in many forms, and the motives behind them are clear: in today's world, there is

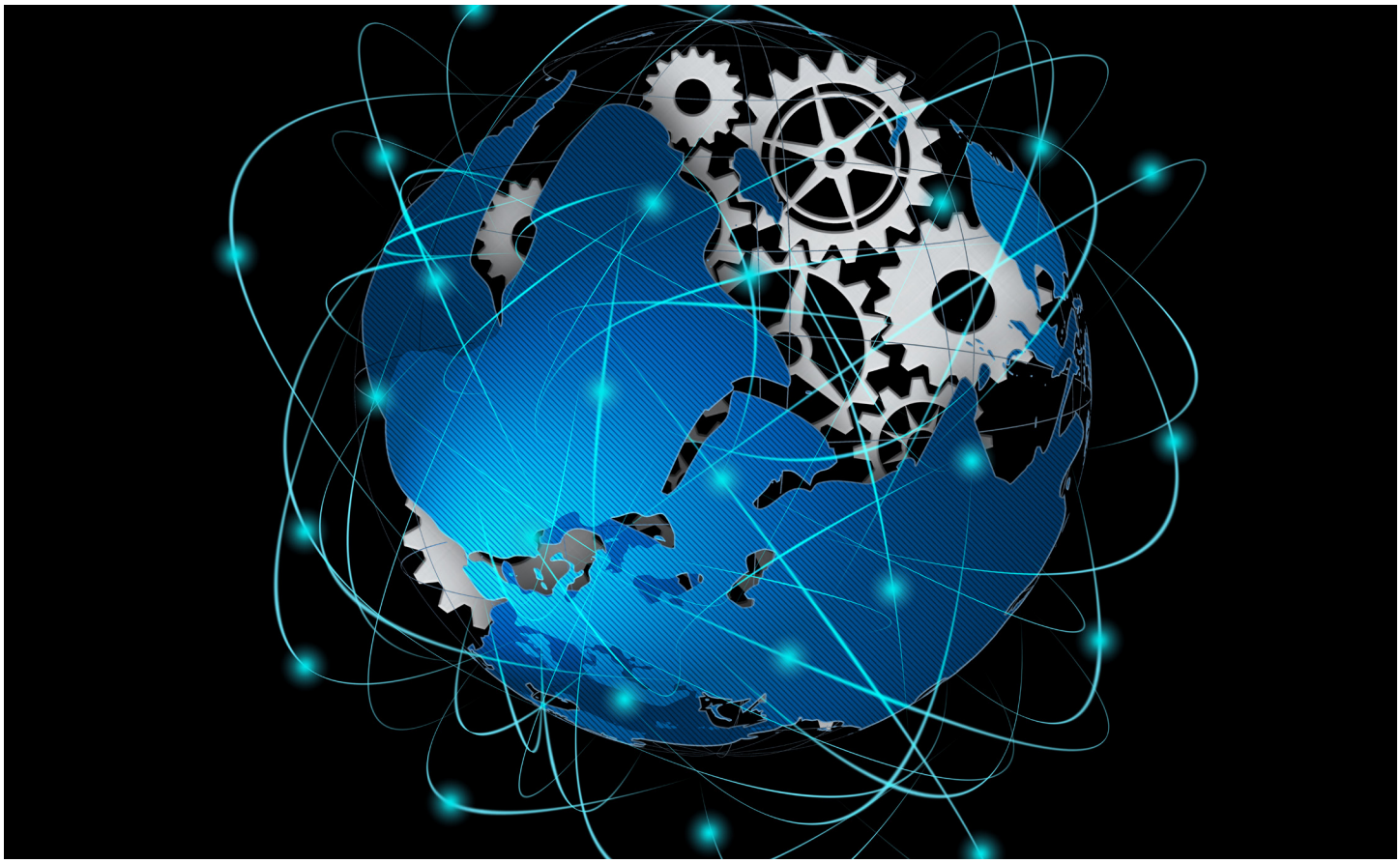
money to be made in stolen data, and lots of it. Statements last year [5] by SEC Commissioner Luis A. Aguilar indicate the market for stolen credit card data alone is $114 billion. Add in the value of other types of data, such as medical information, and even company trade secrets, and it is easy to see why cyber attacks are carried out. Cyber attacks can also be politically motivated or perpetrated by activists.

As long as these motives remain, criminals will continue to carry out cyber crimes. And as our world continues to rely so heavily on computers and networks, with advancements such as the Internet of Things promising even closer connectivity, criminals will innovate and find new ways to launch attacks.

The good news is awareness among businesses is increasing and companies are taking the threat more seriously than ever. Whereas cyber may have been seen as an IT risk historically, it is now generally recognized as an ERM challenge, with the conversation about how to address it elevated to include a company's top executives. In other words, it is becoming clear that cyber risk is business risk.

CYBER RISK AND SUPPLY CHAINS

For a business, recognizing cyber risk within its four walls is one thing, but organizations must also understand this risk in the context of their supply chains — whether they rely on suppliers spread across the globe to manufacture products, or whether they use IT services from a cloud provider. As some have unfortunately discovered, companies can in fact be impacted by a cyber breach along their supply chains. In the 2013 Target cyber breach, for example, attackers got into the system [6] with credentials stolen from an unlikely third-party vendor: an HVAC subcontractor.



A cyber breach along a supply chain can take a number of forms, and affect a company in a number of ways. These varied threats correspond to the major themes discussed previously regarding supply chain trends and risks:

- **Supply chains are becoming more global and more complex,** and, as discussed, since they have become so extended, an event such as an earthquake or major storm suffered at any link in the chain can disrupt the flow of goods or services. The issue, though, does not have to be a natural catastrophe. If a supplier is taken offline by a cyber breach, the net effect is the same.

An attack may not be limited to a supplier's systems, either. A more recent trend shows cyber attacks can cause physical damage at facilities. Reports in January 2015 revealed a steel mill in Germany suffered "massive" damage [7] when a cyber attack disrupted the control system to a blast furnace, preventing it from being properly shut down.

- **Supply chains are becoming more integrated,** which carries both benefits and risks. As Oliver Brew, Aspen's Global Head of Cyber Risk & Head of International Professional Liability, explains: "On the one side, a more integrated supply chain can enable real time communication and efficiencies. On the other side, if systems and networks are more open, then they're more vulnerable."

The danger is that if multiple parties throughout the chain are networked, then, as in the Target breach, attackers can use a supplier or vendor as the point of entry into a company's system. Dr. Chen says many businesses are only beginning to recognize this threat, as the priority has been accomplishing the difficult task of getting systems across the supply chain to talk to one another. "The risk is a fairly recent realization," he says.

- **The liability landscape is being reshaped by supply chains** — as noted, a company could be liable for a defect that originated at one of its suppliers. This is just as relevant for data as it is for products and services. John Mullen, Partner/Chair of the U.S. Data Privacy & Network Security Group at Lewis, Brisbois, Bisgaard & Smith, LLP, explains that the company initially entrusted with customers' data is generally seen as the data owner for purposes of liability and legal duty. This means that while the data may have been passed on to and compromised at a supplier, the initial holder, with some exceptions, will have to respond to a breach.

> "Know your own business. Know where your data is, where you duplicated it, who has access internally and externally — just get a holistic appreciation of where your data sits, moves, and resides."
>
> **John Mullen**, Partner/Chair of the U.S. Data Privacy & Network Security Group at Lewis, Brisbois, Bisgaard & Smith, LLP

Even as businesses take steps to address cyber risks and supply chain risks individually, connecting the dots to identify and address cyber risks within their supply chain is not yet as widespread as it should be. Dr. Chen says news stories about cyber breaches along supply chains catch attention, but as far as prioritizing supply chain cyber risk, he notes, "My sense is it's not very high on the list."

The danger in this outlook, as Dr. Chen points out, is that addressing cyber risk requires constant vigilance. "It's not like a natural catastrophe such as an earthquake," he says. With cyber, you have an enemy on the other side who is constantly improving." Dr. Chen explains that if businesses are not likewise improving as the enemy gets stronger, their vulnerability becomes greater.

ORGANIZATION IMPACTED: TARGET

When: December 2013
Information compromised: 11 gigabytes of data, including names, addresses, phone numbers, email addresses, and payment card information for up to 70 million people.[8]

Key points:

- Successful phishing attack on HVAC vendor.
- Misconfigured systems enabled effective reconnaissance.
- Network segmentation was lacking so that attackers could pivot to point of sale once inside.

ORGANIZATION IMPACTED: OFFICE OF PERSONNEL MANAGEMENT

When: April, June 2014
Information compromised: Birth dates, addresses, and Social Security Numbers of 4.2 million current and former government employees in breach discovered in April; Social Security Numbers of 21.5 million people and 5.6 million records containing fingerprints in breach discovered in June [9].

Key points:

- The very large cache of sensitive data in non-segmented data base created a rich target.
- Appears from first assessment that subcontractor not involved.
- Likely Chinese in origin but hard to measure motive.

ORGANIZATION IMPACTED: RSA SECURITY

When: March 2011
Information compromised: Computer security products used by corporations and governments [10]

Key points:

- Combination of phishing and advanced persistent threat signifies the importance of people of people, not just technology, defense.
- The detection defenses worked, but took time to take effect.

[8] The Target Breach, Two Years Later - ZDNet, November 2015 http://www.zdnet.com/article/the-target-breach-two-years-later/
[9] What to do if you are affected by the OPM data breach - The Washington Post, December 2015 https://www.washingtonpost.com/business/get-there/what-to-do-if-you-are-affected-by-the-opm-data-breach/2015/12/09/534455e0-9dd0-11e5-a3c5-c77f2cc5a43c_story.html
[10] SecurID Company Suffers a Breach of Data Security - The New York Times, March 2011 http://www.nytimes.com/2011/03/18/technology/18secure.html?version=meter+at+1&module=meter-Links&pgtype=Blogs&contentId=&mediaId=&referrer=https%3A%2F%2Fwww.google.com%2F&priority=true&action=click&contentCollection=meter-links-click

PREPAREDNESS AND PROTECTION

Protecting and preparing one organization is challenging enough. Thinking about the potential vulnerabilities along an entire supply chain can seem daunting. There are steps organizations can take though to, at the very least, begin to understand what they do not understand, particularly with respect to sensitive data within the organization and across its supply chain:

- **Know the business** — Many companies do not know what data they hold, where it is stored, who has access to it, or when it is purged, says Mullen. Some companies unnecessarily hold on to old client information or other data that is of little use to them, but may be of value to attackers. Mullen advises, "Know your own business. Know where your data is, where you duplicated it, who has access internally and externally — just get a holistic appreciation of where your data sits, moves, and resides." From there, the process of evaluating how to manage challenges can begin.
- **Protect the company** — Cyber liability insurance is readily available from a number of reputable insurers. While insurance will not prevent a cyber attack, it will help a company recover more quickly in the event of a data breach or network security failure. The key is for companies to consider their insurance needs in the context of the previous step — they must know what they have before they know what to protect. A company may believe it is storing 3,000 records, for example, but learns, upon doing an assessment, it has 3 million records. In that case, the company will need more coverage than originally anticipated. "Get your own ship in order and get enough insurance in place to manage any kind of breach you might face," Mullen advises.

Insurance can cover costs associated with responding to a breach, including investigation, notification, and legal costs. Company executives should speak with an insurance professional regarding what is covered and what is not, and to determine the appropriate coverages. When considering supply chain risk in general, companies should also ask about coverages such contingent business interruption, which covers costs associated with a property loss at a supplier's location.

- **Identify the supply chain** — Businesses should understand that their vendors and suppliers may themselves use subcontractors. The first step toward managing cyber risk in a supply chain is properly identifying the vendors and suppliers within it and knowing who exactly is handling data and how. Sarah Stephens, Head of Cyber, Technology, and Media E&O at JLT Specialty, says creating a system to keep track of vendors is among the first steps a company should take to manage its cyber risk exposure. "You'd be surprised how many companies can't tell you who their vendors are," Stephens says.
- **Set standards and manage network access** — Businesses should create cyber security standards for partners within the supply chain that will be handling data — are suppliers at least the company's equal when it comes to security? Sometimes a company may discover a supplier has more stringent standards than its own — some cloud providers, for example, are as successful as they are because they are more secure and robust than the companies that use their services.

Lauri Floresca, Senior Vice President & Partner at Woodruff-Sawyer & Co., notes that, beyond who holds or manages data, companies should consider which vendors have access to their networks. In some cases, it may be a vendor that should not be expected to be on the cutting edge of cyber security. Floresca notes that the HVAC vendor in the Target breach, for example, would not be expected to have security resources against an

attack. Floresca recommends cordoning off and limiting network access to only what each vendor specifically needs.

- **Negotiate contracts** — To the extent it can, a company should negotiate favorable terms in its contracts with vendors and suppliers. This may be limited by the leverage the company has. A small company using a service from one of the largest cloud providers, for example, will not have much leverage. "But," says Stephens, "where it's more equal, get the best indemnification provisions you can."

Adds Mullen, "If you have power and leverage, you can do audits and have protections in contracts, and be in better shape than most." He says the initial contract between the data owner and the first company in the chain is the most important. If a company has leverage, it can try to put some of the onus on that first vendor in the event of a breach.

Stephens recommends requiring small vendors to carry cyber liability insurance. Beyond the actual coverage protections, she says the underwriting process is usually thorough and sophisticated, and can act almost as a second audit beyond the company's own due diligence when vetting that vendor.

Just as cyber supply chain risks were correlated earlier to broader supply chain trends and risks, the above steps for preparedness and protection can be correlated to the strategies businesses are using to combat broader supply chain risks. Think of identifying and assessing cyber risks associated with vendors and suppliers as the audit programs, where companies gather information about their supply chains and take proactive steps to prevent disruptions. And think of cyber liability insurance and contract terms as a company's way of making its supply chain more robust and able to deal with cyber risks.

When it comes to assessing a company's supply chain, Brew points out, "What is clear, especially for larger organizations, it's near impossible to overturn every stone and look under the hood of every organization you interact with in detail enough to get comfortable with their cyber risk." Since it is not realistic to thoroughly audit every single supplier, companies can stick to consistent principles and identify processes, protocols, and systems to manage weak links.

Floresca says the goal is for a company to understand what rights it has, and to establish clear expectations about obligations in the event of a breach at a vendor: "How they notify you, how you deal with notifying end customers — do you notify or do they? And who pays for that? What audit rights do you have to go into their network and determine what was breached?"

INFORMATION SHARING AND THREAT INTELLIGENCE

Beyond the basic steps companies should take to understand their own organizations, their supply chains, and their respective responsibilities when it comes to data security and breach response, there is a wealth of available information on specific threats that companies can leverage, if they can separate the actionable information from data that cannot be acted on.

Firms such as FireEye offer services to provide companies with threat intelligence — meaningful data on specific cyber threats that are happening in a given industry. The trick is there can be so many data points and not enough resources within an organization to interpret and act on them — this is a lesson one can take from the Target breach, as Target employed FireEye as a threat intelligence source. Obtaining the data is only an effective strategy if a company is able to properly interpret and leverage it.

Stephens separates companies using threat intelligence into three categories: At the lower end are organizations that receive threat intelligence data from a single source. At the higher end, organizations have a dedicated security operation center monitoring real time attacks and cataloging what they see. They then draw lessons they can specifically apply and look at data sources of third-party attacks to gain a fuller picture. Finally, there are organizations that go a step further and look not just at what threats are happening, but anticipate what will happen in the future and examine ways to prepare. Ultimately, companies must make use of what they can, given the resources they have.

As a starting point, Floresca recommends companies work to identify different potential threats and the likely sources of those threats given their specific industry and business, the data they are holding, and their reliance on networks to operate their business. She says companies should ask, "Are threats going to be financially motivated, politically motivated, or carried out by activists? That varies depending on your industry, how visible you are, and what type of information you're holding."

She suggests companies specifically consider: what they need on a day-to-day basis to run their business; how revenue will be impacted if networks are unavailable; to what extent operations can be shifted offline if someone is persistently attacking; whether the network runs a manufacturing facility; what the worst case scenario is that people within the organization can think of, and how the company can recover.

After examining their own business broadly, companies can then get more specific intelligence from expert sources. Keep in mind: information and actionable intelligence are different, and companies must be able to identify the few pieces of information that will actually improve outcomes.

Stephens recommends companies make smart decisions about what security operations they can insource and what they should outsource, keeping in mind how they can bake security into

their outsourcing decisions. “In some cases, for smaller entities, it might be better to rely completely on a managed security provider to manage IT infrastructure, or move basic business processes to a trusted cloud provider,” she says. Larger organizations with better resources and large security teams might do better to insource such operations so they can do a more customized job.

Once a company understands and can leverage threat intelligence, it may consider sharing relevant information among its suppliers and vendors. The challenge is sharing meaningful and actionable intelligence rather than all information that passes through systems. Stephens recommends requiring small vendors to carry appropriate insurance, which for some will be technology professional liability with a cyber component, and for some will be cyber liability insurance.

As Stephens notes, the company is not a managed security provider for its vendors, so it should consider when and how to appropriately share information. Hiring vendors that have effective security capabilities is ideal, but for a subset of vendors with useful services but limited security resources, periodically sending an email advising them about a threat to look out for may be an information sharing strategy companies could employ. As Stephens notes, a buyer of services is not a managed security provider for its vendors, so it should consider when and how to appropriately share information. Hiring vendors that have effective security capabilities is ideal, but for a subset of vendors with useful services but limited security resources, steps like periodically sending an email advising them about a pertinent security threat may be prudent.

COMMON MISSTEPS:

Mullen offers common mistakes he has seen that companies should avoid:

- Companies should not assume because they have a contract that they are protected in the event of a cyber breach.
- Companies should not assume that because a breach is not their fault that it is not their responsibility. "'Not your fault' and 'not your responsibility' are two different things," Mullen says.
- Companies should not try to manage an event — whether the fault lies with them or with a subcontractor — without expert opinion.
- Companies should make sure they use the right experts in the appropriate role. "I see this a lot," Mullen says. "Companies use 'Company X' to support them for security and IT and bring that exact company in for forensics to fix a problem. What if it was their fault?"

REALISTIC GOALS

It is not possible to eliminate cyber risk entirely throughout a global supply chain. Taking steps to limit risk should not be misinterpreted as an airtight defense against threats. But understanding your organization's operations, its supply chain, and its vulnerabilities can lead to the next best thing: resilience, or avoiding the potential for a single point of failure to disrupt your entire supply chain.

Take the first step, if you haven't already, and take measures to understand your operation and your supply chain. Assemble key personnel within your organization to identify how much and what kind of data you are holding and where it sits. Audit your supply chain to the extent you can and protect yourself as thoroughly as possible through your contracts with suppliers and vendors. Speak with your agent or broker about the proper coverages to help protect yourself against cyber threats and other supply chain risks.

The goal is to do all you can to recognizing threats, limit your exposure, and ensure supply chain redundancy.

[1] Stress Test for the Global Supply Chain - The New York Times, March 2011 http://www.nytimes.com/2011/03/20/business/20supply.html?pagewanted=all&_r=1

[2] Toyota, Other Major Japanese Firms Hit by Quake Damage, Supply Disruptions - Reuters, April 2016 http://www.reuters.com/article/us-japan-quake-toyota-idUSKCN0XE08O

[3] All Takata-Made Airbags Without Drying Agent to be Recalled Through 2019 - Autoweek, May 2016 http://autoweek.com/article/recalls/nhtsa-adds-35-40-million-takata-inflators-largest-recall-us-history#ixzz4APz3Vo5x

[4] Apple's Tim Cook Visits Foxconn iPhone Plant in China - Bloomberg, March 2012 http://www.bloomberg.com/news/articles/2012-03-29/apple-says-cook-visited-new-foxconn-plant-in-zhengzhou-china

[5] A Threefold Cord — Working Together to Meet the Pervasive Challenge of Cyber-Crime - U.S. Securities and Exchange Commission, June 2015 https://www.sec.gov/news/speech/threefold-cord-challenge-of-cyber-crime.html

[6] Target Hackers Broke in Via HVAC Company - Krebs on Security, February 2014 http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[7] A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever - Wired, January 2015 https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

DISCLAIMER

For more information, please contact:

Oliver Brew
EVP, Global Head of Cyber Risk
E oliver.brew@aspen-insurance.com

Brian Flynn
SVP, U.S. Head of Cyber Risk
E brian.flynn@aspen-insurance.com
T +1 646-502-1046