From Third to First: A Game-Changing Play in Cyber Risk

July 2017 • Lockton Companies

Cyber risk is a threat that's expanding and shows no sign of relenting. It's unique and unprecedented, but that doesn't mean comparisons and parallels to other risks don't exist. Quite the opposite. Just as property insurance coverage has evolved to meet a changing business landscape, cyber must be considered in a similar context, and that includes addressing cyber as a property coverage issue as well as a liability issue. With its extensive expertise and experience mitigating cyber threats, Lockton is positioned to help enterprises understand their underlying risks in a rapidly changing environment.

This paper will:

- **Outline** the growing cyber threat and demonstrate its ubiquitous nature in the modern-day enterprise.
- **Explain** why cyber risks are increasingly first party that can now lead to damage to physical assets as well as the original data.
- **Describe** the state of the commercial insurance market today in addressing first-party cyber risks as well as the future and investment in underwriting innovation.

AUTHORS

JARED WOSLEGER
Assistant Vice President
Broker
917.351.2528
jwosleger@lockton.com

MAX PERKINS
Senior Vice President
Global Technology and Privacy Practice
011.44.2079332694
max.perkins@uk.lockton.com

PETER ERCEG
Senior Vice President
Risk Solutions
011.44.2079332608
peter.erceg@uk.lockton.com

Estimates put the cyber insurance market at more than **$3 billion**[4] and project it will grow to **$14 billion by 2022.**[5]

Clearly, carriers have the appetite and capacity for the risk.

LOCKTON®

We've Met the Enemy

In the movie *Arrival*, government scientists come face-to-face with extraterrestrial visitors, not knowing if they're friendly or why they've landed on earth. A linguist is brought in to decipher the aliens' language, yet despite her best efforts, she can only translate a few syllables. Armed with this incomplete information, some of the world's most powerful governments react irrationally and mobilize for a military attack.

There are parallels in cyber risk. We're learning more all the time as defenses and protections improve, yet attackers still have the upper hand when there is no mitigation strategy or the strategy isn't carried out. Absent thoughtful mitigation strategies, the odds of making ill-informed decisions will only increase.

Absent thoughtful mitigation strategies, the odds of making ill-informed decisions will only increase.

While general awareness continues to grow with each incident, progress made on the mitigation front is often eclipsed by the failure of companies to move quickly. In this case, attackers are more agile than their target.

The threat is evolving because the spectrum of motivation is widening, and weapons once considered esoteric are more widely accessible than ever.

The threat is evolving because the spectrum of motivation is widening and weapons once considered esoteric are more widely accessible than ever. The actors no longer have only criminal or financial intent but these "agents of chaos" are increasingly sabotaging companies and governments for political and terroristic gain, leaving significant first party damage in their wake.

A cyber attack on Saudi Aramco threatened to cut off a large percentage of the world's oil supply when an employee clicked on a link that released a virus into the company's computer systems. As a result, 35,000 computers were frozen, Internet service went down, and phones went dead. Typewriters and fax machines were pressed into service, and the company had to turn away transport trucks because it lost the ability to make electronic payments.

Hackers seized control of a blast furnace in a German steel mill, causing "massive" property damage, according to reports. At the time the incident came to light, *Wired* magazine warned that attacks on industrial control systems "in the electric grid, in water treatment plants and chemical facilities, and even in hospitals and financial networks . . . could cause even more harm than at a steel plant."[1]

In October 2016, Amazon, Comcast, *The New York Times*, Starbucks, and scores of other large companies were impacted by an attack on DNS provider Dyn. Hackers used a network of infected devices called a botnet to flood and overwhelm Dyn's servers, which rendered many popular websites inaccessible.

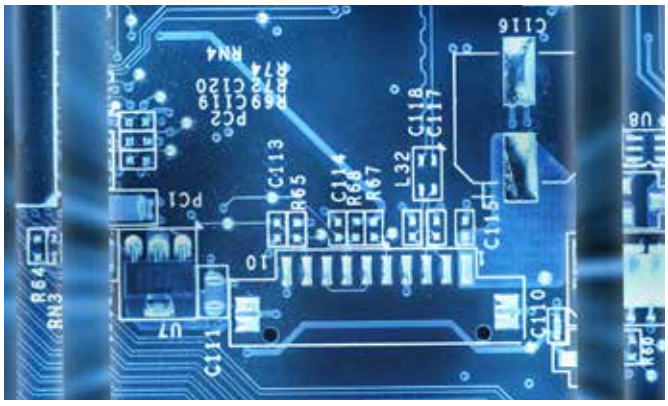
Clearly, the cyber threat is growing as weapons and motivations evolve.

There's strong evidence that for the first time in history a nation-state is employing ransomware.

Britain's security services recently joined a host of other agencies in concluding that the WannaCry outbreak was the work of the North Korean government. In May, 2017 WannaCry seized control of computers operating on Windows 7 that hadn't been effectively patched to prevent such attacks as well as unlicensed and pirated systems that weren't eligible for the patch. The attack infected hundreds of thousands of computers in over 150 countries, demanding payment to release them. Organizations affected included Britain's National Health Service (NHS), Spain's Telefónica, FedEx and Germany's railway system.

Even Distributed Denial of service attacks (DDos), which have been around for years, are also becoming more potent, and even zombie IoT devices driven by botnets now contribute exponential amounts of bandwidth to overload and overwhelm servers with data. Unlike attacks on retailers to steal credit card information, DDoS attacks can cripple an entire enterprise. Instead of draining bank accounts or fraudulently purchasing goods, the intent is to render an entire ecosystem ineffective—or even worse, powerless.

Another emerging threat that's outpacing available defenses is attacks on physical devices and assets. The Internet of Things has improved efficiency in our daily lives; we can control the environment in our home from our smartphones and wearable devices give us actionable health data. In the commercial world, technology is delivering remote control and diagnostic capabilities to big machines—everything from jet engines to industrial controls. Companies that want to improve margins and efficiencies are connecting operational technology (think turbines in a utility) to corporate IT networks and running them remotely instead of with humans. Yet, the efficiency gained through technology is a double-edged sword because the number of significant physical assets at risk for disruption is growing rapidly and most of these devices have few, if any, security controls. If they do, the controls are often left in a default mode, which can easily be defeated by a hacker. With a projected economic impact of $11 trillion by 2025,[2] the attraction of connected devices and machines is irresistible for hackers.



LOCKTON

There's greater transparency on personal data theft because retailers and other industries that handle it are required to disclose a breach to its owners. With respect to attacks on companies motivated by sabotage, for example, it's difficult to know the scale of the threat because companies haven't been required by law to disclose. Yet more will come to light with the increase in regulatory oversight. For example, the state of New York now requires financial services firms to notify the state Department of Financial Services of cybersecurity events, scrutinize the security of third-party vendors, perform risk assessments, and design a cyber mitigation program.

Insurance Market Response

Cyber risk is now one of the most important issues in the boardroom. However, despite the growing attention it commands, first-party consequences are one aspect that has been marginalized or even overlooked.

Cyber risk is no longer confined to liability from handling personal data, but has implications related to property and physical assets that warrant serious consideration.

The evolving nature of the threat is posing a challenge to legacy property policies that were never intended to cover cyber risks and are often silent on whether those risks are covered or not.

Historically, stand-alone cyber insurance products have resided with the financial lines carriers, but when it comes to first-party cyber risk, the insurance market is fragmented. The lines have become blurred as to where coverage starts and stops between insurers. It's difficult for buyers to navigate this relatively new world and know where to find the right product. Although a number of market participants are strongly advocating for cyber insurance to be accessed only through all risks policies, this development is unlikely to occur anytime soon, if ever.

From small businesses to Fortune 500s, every enterprise that uses a computer network has assets that can be compromised by a cyber incident. Some of the first-party consequences of the incidents described above are:

Property damage: Equipment sustains physical damage in an attack. Researchers predict there will be upward of 20 billion connected devices by 2020,[3] and experts agree that critical infrastructure, water, energy, nuclear reactors, and the communication sectors will all be at risk. Property insurance should cover the cost of replacement and installation of equipment as most cyber insurance products exclude property damage.

Network interruption: The insured is unable to operate after suffering a denial of service or phishing attack. This should be treated as a business interruption loss and the insured compensated for loss of income and the increased cost of working around the clock until the network is restored. The majority of cyber insurance products will address this risk, but many property carriers will exclude it based on their consideration of data as an excluded intangible asset and a cyber attack as an excluded peril.

Data corruption: Digital content is damaged, destroyed, or stolen in an attack. A cyber criminal can infiltrate a system through a phishing attack and delete manufacturing code, for example. Besides the Business Interruption consequences, property insurance should cover data restoration costs as a cyber insurance product would.

Theft of intellectual property: The calculation of economic loss is elusive when it comes to theft of intellectual property. This remains an uninsurable risk, as seen when Chinese hackers allegedly stole radar designs and engine schematics for the Lockheed Martin F-35 fighter jet. What remains elusive is how an insurer can model just how much economic damage can be inflicted on a defense contractor by the theft of proprietary confidential blueprints.

Cyber extortion: In this scenario, users are unable to access encrypted data until a ransom payment is made. While the majority of cyber insurers will cover this, it could be argued that this peril would fall under protection and preservation of property where physical property is involved because paying a ransom would restore the IT system and prevent the insured's physical property from being damaged.

Ensuing damage: Coverage for ensuing damage is also an important consideration. An example of this is seen in food processing, where most policies exclude a change of temperature in freezers. However, if hackers gain access to the controls and raise the temperature in a dairy's freezers, an entire inventory of ice cream products can be ruined. Some property carriers would consider this physical damage and are increasingly willing to cover it. Conversely, it's important to note the majority of cyber insurers would not cover this, as ensuing damage is damage to property other than data.

In all of these examples, the adversary has an advantage over the defender.

An attacker only has to be right once, but the defender has potentially multiple physical and intangible assets to protect as well as an ever-increasing attack surface and interdependencies with third parties.

The Internet of Things has introduced more connected devices that can be exposed to a cyber attack; thus, as physical assets, they should be considered by property underwriters.

It's in the Wording

The purchase of insurance to cover first-party cyber risks, particularly to address physical assets, is only now being considered, and it is leading to considerable ambiguity:

- Actuarial data is limited and has minimal relevance in the context of continually evolving threats and attack vectors.
- Large, undefined coverage gaps exist in many property carrier forms.
- Companies have a difficult time defining and assessing the risks they face.

As cybersecurity is now a business risk and no longer simply a technology consideration, insurance brokers play an important role in mitigating physical damage, financial loss and reputational risk. This is where Lockton serves as a trusted advisor to enterprises—helping them identify and articulate their risks and developing strategies. Our approach is differentiated in that we mobilize experts from across the insurance spectrum who understand cyber, liability and property so every possible consequence and outcome is addressed and properly mitigated for our clients. Our expertise is complemented by new insurance products which address the gaps in legacy property and casualty policies, known as Difference in Conditions and Difference in Limits policies.

Often, business interruption and denial of service are covered, but as far as ensuing perils are concerned, there's no uniformity among carriers. Understandably, many property underwriters have only limited experience with cyber and, therefore, find it difficult to classify data as "property." This represents an opportunity for risk managers and brokers to work toward a deeper understanding of the data that exists in enterprises and how that data impacts the risk.

The Technology Solution

Much has been written about the challenges of underwriting cyber risk for insurers, in particular catastrophe modeling for cascading losses from single events as well as insufficient actuarial data. A common theme is the lack of understanding of how an investment in specific controls moves the risk needle in a constantly changing threat environment. However, thanks to new partnerships and mindsets we can feel more confident about our ability to get ahead of the problem. Technology is playing an increasingly important role in our advancement and the insurance industry has a powerful ally in tech startups.

Just as linguist Louise Banks ventured into the belly of the beast to better understand the extraterrestrial visitors in *Arrival*, a rapidly growing league of intrepid investigators is exploring new frontiers. Deeper data analytics that promise to accelerate our understanding of cyber risk are emerging, as Silicon Valley firms join insurers and brokers to develop tools to evaluate an enterprise's security position from the inside and the outside. Traditional underwriting processes offer only a snapshot in time in a dynamic and fast-moving risk environment.

Technologies that help insurers evaluate risk in real time are supporting many more underwriting decisions today and, over time, will evolve to influence how these risks are priced.

In a nation where 80 percent of the critical infrastructure is owned by the private sector and beyond the purview of effective government regulation, technology innovation driving rigorous enterprise risk management will become the best way to improve mitigation and protect valuable assets such as data, intellectual property, and machinery.

> Cyber risk is certainly insurable, but in many respects, it's the new asbestos.

Conclusion

Cyber risk is certainly insurable, but in many respects, it's the new asbestos. Its reach appears to be infinite. It's also an existential threat to business, where one event can cause multiple losses in unanticipated ways. This is due, in part, to the fact that the cyber threat has been shown to have a growing impact on physical property. In this instance, it would be advisable to adopt a historical context and acknowledge the parallels to the evolution of property insurance. Just as the introduction of fire protection systems transformed underwriting of physical property, so should risk managers, brokers and insurers reevaluate physical assets in the context of cyber.

Addressing cyber risks as a property issue is a relatively new concept, which is why there is ambiguity in the insurance marketplace. Aggressive action needs to be taken because the risks are propagating at an alarming rate. The insurance industry must innovate so it remains an indispensable business partner to clients who have a lot riding on protecting their financial performance, reputation, and sustainability.

---

[1] A Cyberattack Has Caused Physical Damage for the Second Time Ever, *Wired,* January 8, 2015

[2] Unlocking the potential of the Internet of Things, McKinsey & Company, June 2015

[3] Press release: Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015

[4] Cyber insurance market to see rapid growth through 2022, *Business Insurance,* December 7, 2016

[5] Cyber Insurance Market—Global Opportunity Analysis and Industry Forecasts, 2014-2022, Allied Market Research

LOCKTON®

lockton.com