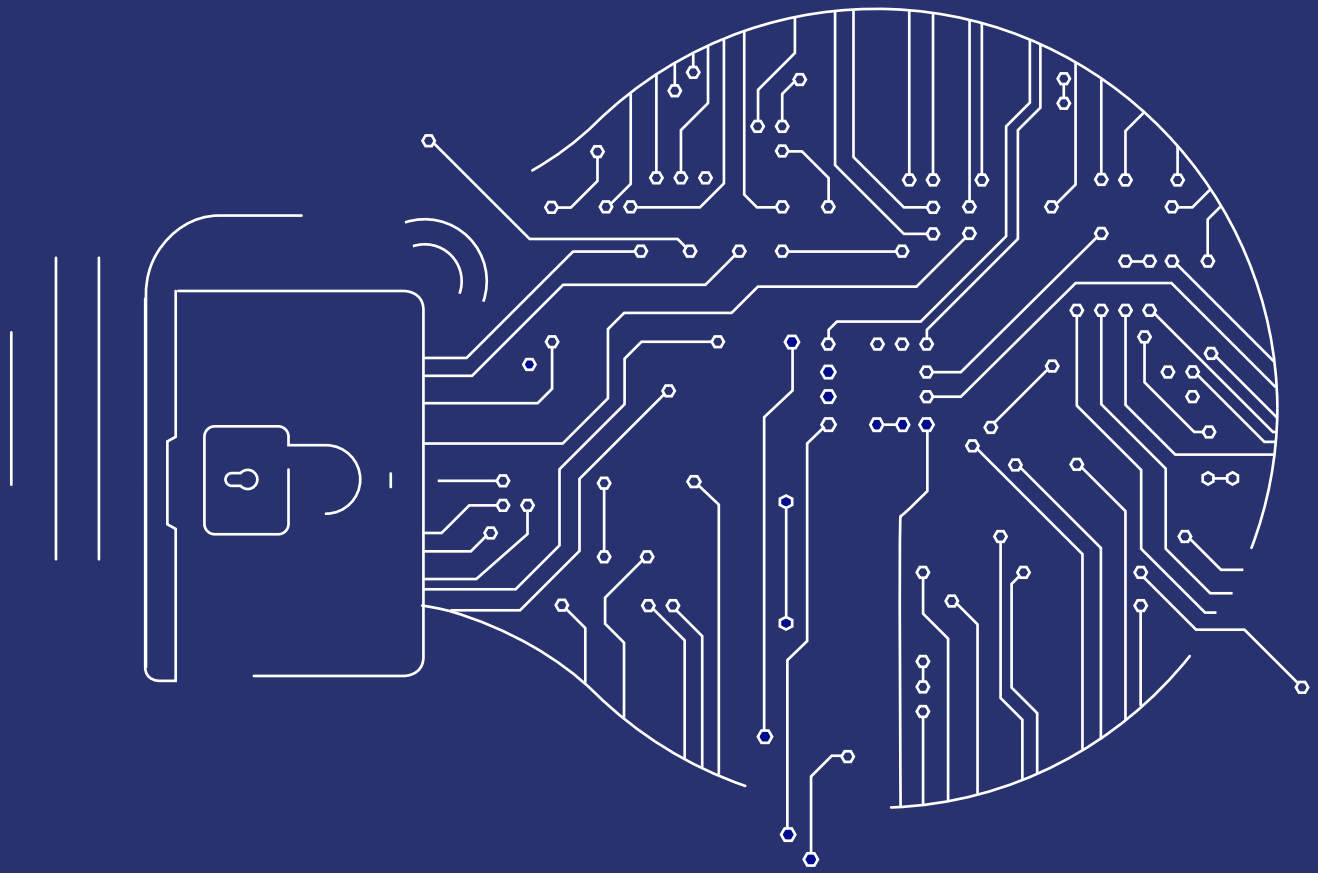
Cyber and Business Interruption Risks:
Connectivity Adds Complexity



CLYDE&CO

North American Cyber and Business Interruption Risks:

Connectivity Adds Complexity

Interconnectivity has always presented opportunities and risks for global businesses. On the one hand, greater connectivity facilitates global commerce. On the other, it increases organizations' exposure to disruptions. The near-universal reliance on technology and internet access have made disruption and data loss particularly worrisome for businesses - and their insurers.

In an era where a majority of the world's population is online, cyber incidents that sever or slow connectivity have emerged as a significant source of business interruption for businesses in North America and, indeed, globally.

For the insurance industry, this is a complex issue, because insurers do not have a uniform approach to covering such scenarios, and there is a dearth of case law regarding cyber coverage under all-risks policies in the United States and Canada. As a result, business interruption caused by cyber events may become a major area of claims litigation in the Americas.

Despite this, mitigating business interruption in all its forms (whether from natural or human causes) remains an area of opportunity for corporate insurance buyers as well as insurers. For midsize and small organizations, business interruption can be financially devastating; if they experience such a shutdown without insurance, some may never reopen. Insurers have a vast and diverse set of risks to assess, and their role in business resilience is critically important. This paper will examine the growing impact of cyber risk in business interruption claims and evolving forms of physical damage that cause financial loss. For insurers, where there is risk, there is opportunity.

Issues in business interruption

Supply chains have been vulnerable to natural catastrophes for as long as such links have existed. As businesses stretch their supply chains across the globe, points of potential weakness increase, as does the risk of disruption from fire, wind and water. Traditionally, property business interruption is insured under time-element coverage in all-risks policies. Such coverage generally responds to losses arising from named perils, and physical damage is a condition precedent to coverage. Today, however, the nature of supply chains has evolved, and the events that can damage or destroy those connections have grown more complex.

Greater complexity in supply chains presents its own set of challenges. More businesses rely on suppliers that are based in different jurisdictions. Contingent business interruption insurance – designed to pay for income loss and expenses resulting from damage to a supplier or, in certain instances, a customer – has been available for many years. Typically, damage to the supplier's property is required to trigger this coverage.

But US courts have held that physical damage is not always required to trigger coverage. In fact, two types of supplemental business interruption coverage can provide protection in such a circumstance:

Ingress/egress

Restricted access to a business can cause loss of income even when the business facility itself does not have physical damage. For example, if a hurricane or flood blocks all roads leading to the business, it may be impossible for employees and/or customers to reach the premises. Unable to produce or sell its wares at its normal operating capacity, the business is likely to lose income. In *Fountain Powerboat Indus. Inc. vs. Reliance Insurance Company*, 119 F. Supp. 2d 552 (E.D.N.C. 2000), the US District Court for the Eastern Division of North Carolina ruled that the ingress/egress clause of a business interruption policy covered the policyholder's income loss from reduced manufacturing capacity after Hurricane Floyd made access to its facility impossible.

Civil authority

This coverage applies to loss of income from restricted access that results from orders of civil authority. An example is loss of business income during a curfew imposed by a city or state in response to civil commotion. In *Sloan v. Phoenix of Hartford Insurance Company*, 207 N.W.2d 434 (Mich. Ct. App. 1973), the Michigan Court of Appeals affirmed a trial court ruling that a business interruption policy covered the policyholder plaintiff's loss even though its facility did not have any physical damage.

Cyber risks are not always physical

Today, the insurance industry is grappling with the challenge of providing coverage where the source of interruption comes from alphanumeric code rather than nature's fury, where financial loss can be significant, though physical damage is not easy to observe. This scenario is not uncommon for organizations whose businesses rely on computer networks and internet connectivity. Access to data has become the lifeblood of commercial enterprises.

A loss of access and/or data itself can quickly result in lost revenue. Whether caused by malevolent or inadvertent actions, even disruptions of short duration can be quite costly. Consider the following examples:

Network outages

In 2016, Delta Air Lines suffered a crippling network outage, lasting 6 hours and costing the airline USD 150 million in lost revenue. The system-wide network outage was caused by a power failure and forced the airline to cancel or delay flights worldwide.

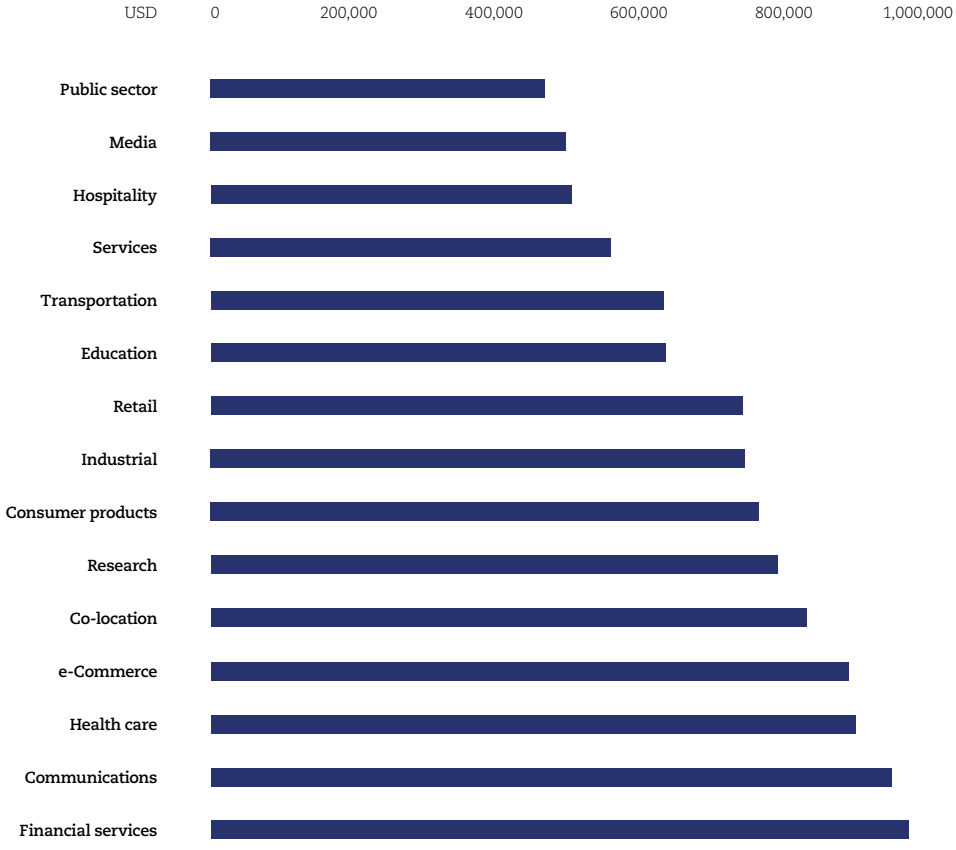
Air Canada experienced a nationwide network outage during a busy vacation period in March 2018 that affected travelers at airports around the world. The airline not only faces loss of revenue, but it incurred costs too – such as those involved in having to issue handwritten boarding passes to some passengers during the outage.

A 2016 study by the Ponemon Institute found that the average total cost per minute of an unplanned outage at a data center was USD 8,851. According to Ponemon, the average duration of a total shutdown was 130 minutes. The average cost of a total data center outage was USD 946,788.

Network outages costly to industries

Total cost of a single unplanned outage by industry

Source The Ponemon Institute, 2016



Cyber infrastructure attacks

A distributed denial-of-service (DDoS) attack in October 2016 on the organization that administers a key element of the World Wide Web took down sites including Twitter, PayPal, Amazon, Netflix and others. The organization, known as Dyn and now part of Oracle Corporation, administers the Domain Name System (DNS), which translates site names into numeric addresses – a critically important method of accessing servers on the internet. While denial-of-service attacks directed at individual sites and DDoS attacks tend to be temporary, other forms of cyber attacks can do lasting damage.

Automated services businesses are particularly vulnerable to disruption from cyber attacks, which can cause a host of problems, from loss of data to property damage and even personal injury. Canadian energy and mining companies, which operate automated drilling and production systems, warn that cybersecurity attacks could hack such systems and wreak havoc.

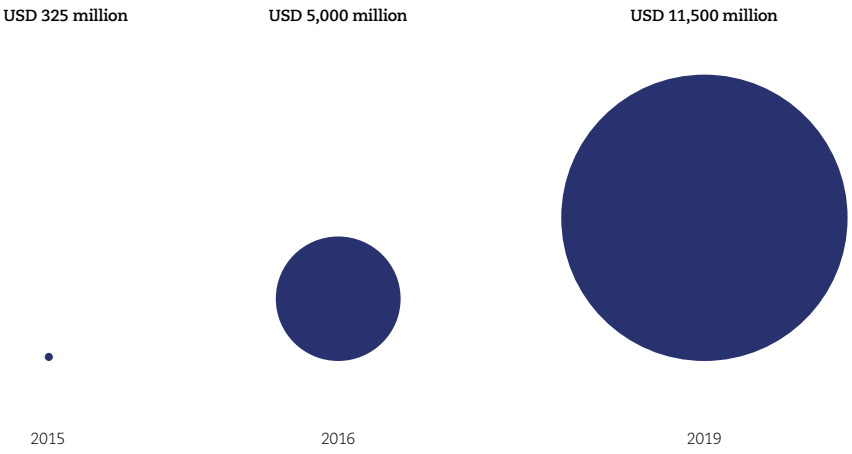
Ransomware

Cyber attacks that encrypt data in an attempt to extort money from victims are becoming a more frequent threat. During 2017, two massive malware attacks (known as Wannacry and Petya) affected hundreds of thousands of computers in more than 150 countries. These attacks and variants were responsible for disruptions at the United Kingdom's National Health Service, Danish shipping company Maersk, Germany's national railway, food packaging giant Mondelez and other large organizations. An even more sinister form of attack may masquerade as ransomware but is more accurately described as "wiperware." This form of malware destroys data, damages hardware and makes system recovery much more difficult. Maersk reported that the 2017 malware attack would impact its financial results by up to USD 300 million. The risk of disruption from ransomware is soaring. According to the Federal Bureau of Investigation, more than 4,000 ransomware attacks occurred each day in 2016, four times as many as the year before.

Ransomware costs to soar

Estimated damage costs,
in millions of USD

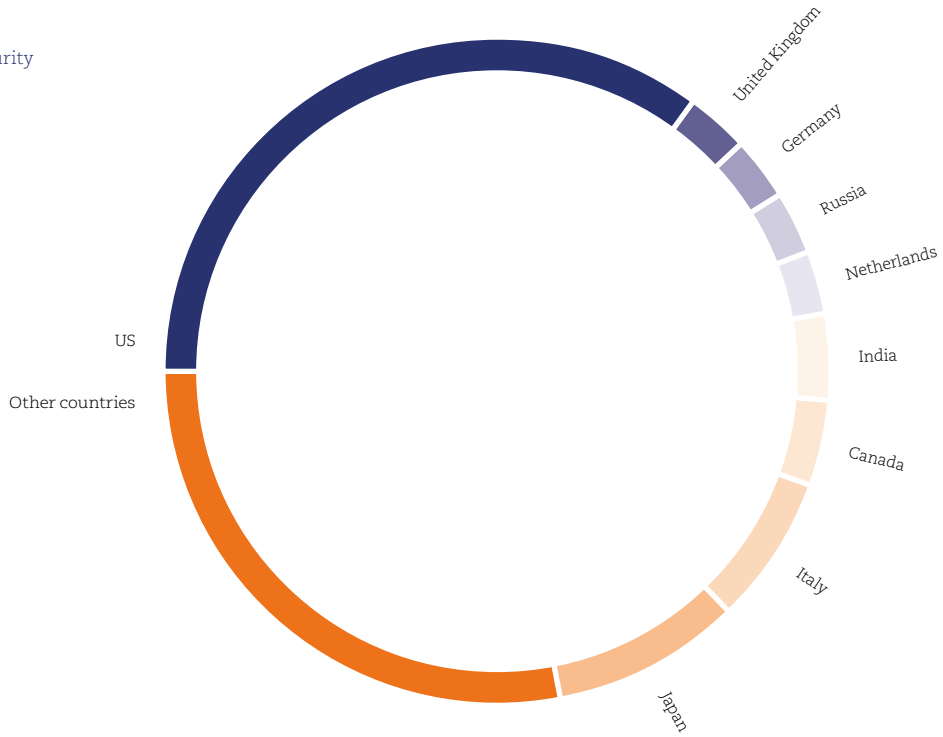
Source Cybersecurity Ventures



Ransomware: a global menace

Percent of antivirus detections
by country, 2016

Source Symantec, "Internet Security
Threat Report 2017"



Coverage considerations

> “Some coverage for business interruption is emerging in cyber liability policies, and a handful of insurers are testing this coverage in the marketplace.
>
> **– Christina Terplan, Partner**

Historically, coverage for business interruption has been provided through property policies and responds to physical damage to tangible property arising from named perils. Those perils traditionally have included fire, windstorm, earthquake and the like. Time deductibles and indemnity periods under such policies vary. A common time deductible, or waiting period before business income loss coverage begins, is 72 hours.

For income loss from property damage due to natural catastrophes such as hurricanes, which can develop over several days, such a period is reasonable from the underwriter’s point of view. But a three-day timeframe is disproportionately long when applied to a cyber event, notes Christina Terplan, a Clyde & Co partner based in San Francisco.

“Cyber coverage waiting periods are typically eight hours. Longer could be catastrophic for the insured,” Terplan says.

“Some coverage for business interruption is emerging in cyber liability policies, and a handful of insurers are testing this coverage in the marketplace,” she says. “Features of these new policies include triggers aligned with the reality of reliance on computer networks. For example, shutdown is no longer necessary as a trigger. Instead, system slowdown can be a covered event,” Terplan explains.

Business interruption and contingent business interruption coverage are provided under three types of policy forms:

1. **Insurance Services Office (ISO) forms**

   ISO forms, commonly used in the United States, typically are more restrictive in their coverage terms, particularly regarding electronic data. For example, ISO form 00 32 10 12 (Business Income and Extra Expense) states: "Coverage for Business Income does not apply when a 'suspension' of 'operations' is caused by destruction or corruption of electronic data, or any loss or damage to electronic data, except as provided under the Additional Coverage, Interruption of Computer Operations." The additional coverage is subject to a sublimit in the ISO form.

2. **Proprietary insurance company forms**

   Company forms usually are less restrictive than those using ISO wordings. Proprietary forms may include new coverages for cyber risk, for example.

3. **Broker or manuscript forms**

   These forms generally provide the broadest coverage for business interruption.

As insurers look for ways to differentiate their products and respond to market needs, some companies are offering data restoration coverage if data becomes corrupted or deleted.

Lack of clarity

> “The policy language has not yet caught up to the current realities of cyber risk.
>
> **– Robert W. Fisher, Partner**

Definitions matter when it comes to policy wording. At the moment, there is little clarity regarding coverage for cyber events in business interruption policies, points out Robert W. Fisher, a Clyde & Co partner in Atlanta who specializes in first-party property insurance coverage issues.

“Physical damage is relatively straightforward. Non-physical damage is murky,” Fisher says. In many quota share programs there is “a lack of concurrency among insurers’ wordings relating to cyber risk. The policy language has not yet caught up to the current realities of cyber risk.”

Questions that are without definite answers, Fisher adds, include: “When does a cyber attack touch a property policy? Can an electronic event become a physical damage event?”

Fisher and Terplan both assert that computer systems can be compromised and rendered permanently unusable. Cyber underwriters, however, generally do not want to cover hardware, Terplan adds.

In Canada, there is a scarcity of case law regarding cyber insurance, and even fewer cases involving coverage of data loss under property policies, notes Nathalie David, a partner at Clyde & Co in Montreal. “These issues are likely to be debated in the coming years. Cyber incidents are increasing in frequency for Canadian organizations, and business interruption will become part of that trend.”

Lack of clarity leaves the door open to disputes

The lack of clarity and concurrency in US and Canadian insurance policies may leave open the door to coverage disputes. At a minimum, there is a need for the insurance industry to develop a framework for coverage that is intended to respond to cyber risk and business interruption.

Further complicating matters is the fact that US courts are divided on whether cyber incidents such as data loss constitute physical damage.

In *Ward General Insurance Services Inc. v. Employers Fire Insurance Company*, 7 Cal.Rptr. 3d 844 (Cal. Ct. App. 2003), the California Court of Appeal ruled that a business property policy did not cover the loss of electronic data when the policyholder's database crashed during an update due to human error. The court wrote in its opinion, "We fail to see how information… can be said to have a material existence, be formed out of tangible matter, or be perceptible to the sense of touch." Further, the court concluded that "the loss of the database, with its consequent economic loss, but with no loss of or damage to tangible property, was not 'a direct physical loss of or damage to' covered property under the terms of the subject insurance policy, and, therefore, the loss is not covered."

The Court of Appeals of Texas, however, in *Lambrecht & Associates Inc. vs. State Farm Lloyds*, 119 S.W.3d 16, 25 (Tex. App. 2003), found that a policyholder was entitled to business interruption coverage for its loss of computer data after its computer system was hacked. The Texas appellate court reversed the trial court's judgment that the loss of data did not constitute a physical loss.

In general, there is little case law on whether economic losses from cyber events are covered under all-risks policies, David, Terplan and Fisher note. In addition, insurance policies vary on whether they exclude cyber and loss of electronic data.

"Canadian policies for various sizes of organizations tend to embed coverage for business interruption and cyber risks. We see a bit of everything in policies," David says. "US litigation trends are always a factor that Canadian insurers consider, however. Even though it typically takes some time, large carriers and leading market companies will often base themselves on the experience of their US counterparts to develop the next wave of insurance products in Canada."

Two cases have addressed the issue of whether loss of use of computer systems constitute physical damage under all-risks policies. In *American Guarantee & Liability Insurance Company v. Ingram Micro Inc.*, 2000 WL 726789 (D. Ariz. April 18, 2000), the trial court found that physical damage "is not restricted to the physical destruction or harm of computer circuity, but includes loss of access, loss of use and loss of functionality." A Tennessee district court in *Southeast Mental Health Center Inc. v. Pacific Insurance Company*, 439 F.Supp. 2d 831 (W.D. Tenn. 2006) found that the policyholder was entitled to coverage under its all-risks policy for the loss of data from its computer system, which was damaged during severe weather. The Tennessee court ruled that the plaintiff's loss of income stemming from its inability to use its computer system was covered under the policy.

Conclusion

Business risks and the insurance products that address them often outpace case law on coverage issues. On the topic of cyber risk in business interruption, what is at the moment an underwriting issue has the potential to transform into coverage disputes – and more litigation. In the meantime, risk professionals, their advisers and insurers can all take action to mitigate the risks.

When it comes to purchasing cyber and business interruption coverage, policyholders and brokers should engage underwriters and openly discuss both their needs and concerns. Insurers should clarify their coverage intentions and examine their wordings in both cyber and business interruption policies. As underwriters and claims departments see more incidents involving cyber occurrences, there may be opportunities for growth through blended coverage products. Dialogue between insurers and their insureds on cyber and business interruption can bring clarity and promote innovative solutions to a thorny problem for businesses and the global insurance industry.

Christina Terplan
Partner, Clyde & Co

+1 415 365 9821
christina.terplan@clydeco.us

Robert W. Fisher
Partner, Clyde & Co

+1 404 410 3153
robert.fisher@clydeco.us

Nathalie David
Partner, Clyde & Co

+1 514 764 3611
nathalie.david@clydeco.ca

50
Offices

3,600
Total staff

390
Partners

1,500
Lawyers

www.clydeco.com

J421469 April 2018