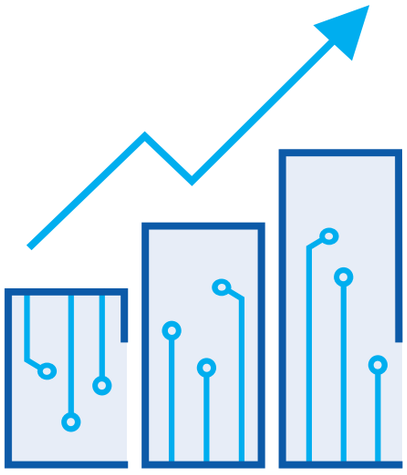


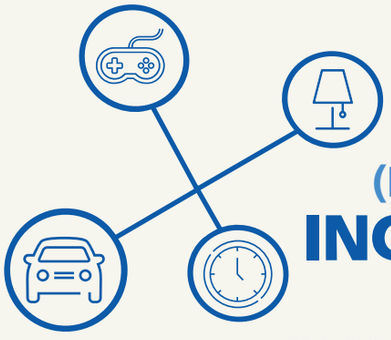
CYBER RISKS ARE GROWING

BUT BUSINESSES CAN DEFEND AGAINST THEM

The risks to businesses large and small posed by today's sophisticated cybercriminals are increasing by the day.

OVER 10.5 BILLION MALWARE ATTACKS DOCUMENTED IN 2018.[1]

391,689 NEW MALWARE VARIANTS WERE IDENTIFIED IN 2018.[1]



INTERNET OF THINGS (IOT) ATTACKS **INCREASED 217%** IN 2018 OVER 2017.[1]

MOBILE RANSOMWARE INFECTIONS **INCREASED 33%** OVER 2017.[2]

OFFICE FILES ACCOUNTED FOR **48% OF MALICIOUS EMAIL** ATTACHMENTS IN 2018, UP FROM ONLY 5% IN 2017.[2]

71% OF 2018 RANSOMWARE ATTACKS TARGETED SMALL BUSINESSES.[3]

1. "2019 SonicWall Cyber Threat Report: Unmasking the Threats that Target Global Enterprises, Government & SMBs." SonicWall. 2019.
2. 2019 Internet Security Threat Report. Symantec. Volume 24. February 2019.
3. Davis, Jessica. "71% of Ransomware Attacks Targeted Small Businesses in 2018." 27 March 2019. HealthITSecurity.com.

Helping companies understand and protect against the expanding, global threat of cyber risk

Unlike the teenage hackers of yesterday, today's high-tech pirates attack for profit, and business is booming. Globally, ransomware attacks, "cryptojacking" of digital assets and new malware variants aimed at mobile devices are on the rise. According to one cyber risk watchdog, a theoretical, international ransomware attack might have a global price tag of over $193 billion, with up to $89 billion of that tab landing at the feet of the American economy.[1]

U.S. and global companies must operate within this environment every day, but they are not without allies. The global insurance industry is developing products and tools aimed at helping companies better understand, assess and mitigate cyber risks. LEADERS recently spoke with three of Zurich's top cyber risk underwriting executives to hear their perspectives on the growing threat and how their company is helping clients protect against it.

An evolving threat

Lori Bailey
Global Head
of Cyber Risk
Zurich Insurance Group

How would you characterize the current state of global cyber risk?

Cyber risk is evolving constantly, not only because technology is advancing so quickly, but also because the threat actors are keeping pace with technological change. Organizations are utilizing advanced technologies to become more efficient in their business operations. However, that efficiency may come at a price, since unanticipated vulnerabilities of new technologies could be readily compromised by threat actors.

In addition, risks are heightened because cyber regulations are also evolving globally. In the United States, regulations are likely to become even tighter in the wake of the GDPR adopted in Europe last year – something which we are already seeing with the passage of the California Consumer Privacy Act (CCPA) scheduled to go into effect in January 2020. Similar laws are going into effect in Brazil next year, with other countries adopting language similar to the GDPR. As technology and cyber threats continue to evolve, new regulatory guidelines will come into play following cyber events. Businesses will be faced with the conundrum of adopting new technologies that can enhance their operations, but may expose new threat vulnerabilities and draw closer scrutiny under tightening regulatory frameworks.

What were some of the key cyber risk findings in the World Economic Forum's 2019 Global Risks Report?

One of the biggest changes over the last several years is that cyber risk now consistently ranks in the top five global risks in terms of likelihood. The overall impact is still somewhat undetermined because cyber events can impact different organizations in different ways. But cyber risks consistently pop up in the top five most concerning risks.

Ransomware has been making a lot of headlines of late. Is the threat growing?

The threat is definitely increasing, but as a whole, ransomware attacks are often underreported. Companies that don't have insurance may simply pay them out. The downside is you may not get the decryption key you need to get your data back. Similarly, you've also indicated that you are willing to pay, so you could be a victim again. I see ransomware attacks continuing to increase as threat actors become more sophisticated and the value of cryptocurrencies remains high. And as long as companies are willing to pay these kinds of attacks will continue in the future.

What keeps you awake at night when you think about the future of cyber risk?

Certainly, cyber terrorism and state actors are growing concerns, including attacks on critical infrastructure, financial institutions, water supplies and utility grids. These are attacks that can not only cause financial disruption, but also physical damage and bodily injury if taken to extremes. That's what keeps me awake almost every night.

1. Major ransomware attack could hit U.S. with $89B in economic damages. Cision PR Newswire. 29 January 2019.
2. Framework for Improving Critical Infrastructure Cybersecurity - Version 1.1. National Institute of Standards and Technology (NIST). U.S. Department of Commerce.16 April 2018.

THE FIVE CORE FUNCTIONS OF THE NIST FRAMEWORK [2]

The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, recommends building a cybersecurity framework around the following five steps:

IDENTIFY
"Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities."

PROTECT
"Develop and implement appropriate safeguards to ensure delivery of critical services."

DETECT
"Develop and implement appropriate activities to identify the occurrence of a cybersecurity event."

RESPOND
"Develop and implement appropriate activities to take action regarding a detected cybersecurity incident."

RECOVER
"Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident."

Insuring the risks

Michelle Chia
Head of Cyber and Professional Liability
Zurich North America

Despite what appears to be growing awareness of cyber risk, do businesses fully understand the scope of the threat?

I would say that many companies are still not as sophisticated as they need to be around this topic. Hence, they are not as well versed as they could be about cyber threats and how to protect themselves. Education is the key. That's why Zurich has partnered with organizations like the World Economic Forum. In 2018 and 2019, the WEF Global Risk Report stated that large-scale cyberattacks are among the leading risks in likelihood and impact. Educational opportunities like that report and other vehicles can help to increase the business community's understanding of cyber risk.

Are smaller companies at greater risk than large firms?

I want to emphasize that vulnerability to cyber risk is not size-dependent. We're all at risk, regardless of size. However, midsized and smaller companies tend to have fewer resources to protect themselves. And because the world is so interconnected, there can be a domino effect when a threat enters the network of one organization and is able to spread through connections with other businesses, such as suppliers or customers. Because all companies operate in the same cyber ecosystem, what impacts one company can ultimately affect others. And the threats are evolving and changing at an accelerating pace all the time.

How are cyber insurance policies responding to those evolving risks?

Cyber insurance policies need to be updated constantly to be able to respond to the most recent types of events. Zurich did a major refresh of our standalone cyber policy at the end of last year. We are able to stay current with developing cyber risks because we have a dedicated underwriting team focused on understanding the exposure and line of business.

Can cyber coverages be customized to the risks of specific industries?

Yes, we are working to build out coverages unique to specific industries. For example, we've created an endorsement targeting the construction industry. Historically, construction has not been seen as high-risk because it was not as data-intensive as other industries. But contractors are adopting a lot of new technologies. Construction is one of a handful of industries where the use of drones is becoming more widespread. This could mean privacy claims resulting from drone usage. We are also broadening the definition of computer equipment to include wearable safety devices provided to construction workers. While these devices increase worker safety, the technology behind the equipment can create new cyber risks for employers. We are looking to build out other industry-specific endorsements that really speak to the language and the unique needs of companies in other industries.

How is Zurich helping customers address today's intensifying cyber risks?

We have entered into a business relationship with a well-known cybersecurity provider that does monitoring and mitigation services for Zurich customers when they purchase our cyber policy. The company has extensive experience in helping both the government and commercial organizations identify the threats they are facing and ways to mitigate or eliminate the threats. Zurich also has an experienced and very capable, dedicated Cyber Risk Engineering team to help figure out what gaps may exist to help Zurich customers develop effective cyber risk response plans. We are constantly researching the risks facing our customers, helping them deal with the ones we know and preparing them for what may be on the horizon.

The underwriting view

Yosha DeLong
Technical Director – Cyber and Professional Lines
Zurich North America

How do cyber insurance policies differ from traditional property and liability policies?

Traditional liability and property policies were written to cover conventional bodily injury claims and property losses. Cyber wasn't an issue when these policies were developed. When insurers originally began to write cyber policies, the first were designed to cover data breaches and the associated state-required notification and regulatory aspects. When the industry started writing this exposure 10 or 15 years ago, what we were seeing most often were laptop-related events, not these malicious, large-scale attacks we see now.

The kinds of threats companies are experiencing today were not even contemplated when these policies were created. We've seen a real evolution in cyber risk with the advent of ransomware and other kinds of malware that have the potential to cause significant business interruption and reputational damage.

Are cyber exposures more challenging to insure than traditional risks?

Well, some people within the insurance industry get worried when you talk about underwriting cyber because they don't believe that our industry knows the technology well enough. But the foundation of underwriting cyber is much the same as any other commercial insurance contract. You look for the facts, weigh the possibilities and map out the potential scenarios, and then make an underwriting decision based on your best information and judgment. Good risk selection is at the core of being a successful underwriter in any aspect of insurance. The main challenge in underwriting cyber risk is the continuously changing nature and scope of the threat.

For example, five years ago a lot of retail organizations got hit hard by cyberattacks. Since then, they have really changed the way they handle credit cards. That has changed the exposure for the better, at least on that aspect of the risk. On the flip side, five years ago we saw manufacturing as an easy risk to write for cyber because they didn't have large amounts of data. Now, with the business interruption implications of vendor and supplier connectivity and greater reliance on information technology in all aspects of construction, there is a huge potential for disruption if someone gets into the network and initiates a shutdown or ransomware event.

Does Zurich use any special tools in the cyber risk selection process?

Yes, we do. We have a service provider called Cyence that performs data aggregation using publicly available information about potential customers and then applies an algorithm to help determine the risk quality. It's in line with what property underwriters have been doing for years with the information provided by Risk Engineering visits.

One of the factors we must consider when underwriting cyber is that it is always a truly global risk. In property insurance, you can gain a view of your risk accumulation based on where your book of business is concentrated, such as the east coast of Florida for windstorm. Cyber isn't like that. When an event happens in the U.S., it can quickly become a global event due to the universal network connectivity. We can't view cyber risk in regional pockets like property and pretend we have a complete view of the potential scope of an event. An event can go global overnight.

I can say that the insurance industry is deeply committed to helping our customers protect against this risk. We will continue to work with customers to develop solutions both for the known cyber risks of today and the unknown ones that lie ahead.

THE MORE RISKS YOU SEE, THE SAFER YOUR BUSINESS CAN BE.

Be more proactive about protecting the business you love by expanding your risk horizons. Zurich's risk profiling is a structured approach that helps identify, prioritize and mitigate risk. We can help you manage your risk rather than just insure against it, so you can focus more on profit and less on risk.

VIEW OUR RISK PROFILING VIDEO AT zurichna.com/rp2

ZURICH INSURANCE.
FOR THOSE WHO TRULY LOVE THEIR BUSINESS.

ZURICH®