Expanding connectivity means new opportunities for innovation, but also openings for cyber risk

One of the most significant technological innovations of the 21st century, the dawning of the "Internet of Things," is reshaping our professional and personal lives in ways once limited to the realm of science fiction. According to one estimate, the number of web-connected devices will swell to more than 75 billion by the year 2025[1]. And for businesses, any one of these connections may represent an unanticipated avenue for hackers and even nation state actors to launch malware that can disrupt networks, supply chains, business operations, and even critical infrastructure.

When most people think about security breaches their concerns usually focus on the possibility of personally identifiable information being stolen by hackers. While those threats are still very much with us, C-suites today must come to terms with cyber risks that can originate from almost any direction, representing a strategic risk with a real ability to threaten business continuity.

"From a business perspective, it's no longer just those industries that have a lot of personally-identifiable information that need to think long and hard about cyber risk, like financial services or retail," said Zurich's Global Head of Cyber Risk **Lori Bailey**. "It's every industry now – automotive, industrial, agriculture, transportation and utilities. CEOs in traditionally less-data-intensive industries can no longer say 'We're not a tech company, so we don't have to worry about this to the same degree.' The societal and economic impacts caused by widespread disruptions due to viruses or malware can have global implications."

Bailey noted that the "WannaCry" attack of 2017 was a major wake-up call for many organizations around the world. What made that cyber event so unusual was that it did not simply attack one specific industry or organization. Instead, it impacted a specific vulnerability in an operating system used by a broad diversity of companies, having a far-reaching effect on many industries with the potential for significant business interruptions.

The potential for business interruptions introduced by the growing online connectivity of devices supporting critical infrastructure, such as public utilities and transportation systems, is prompting a growing awareness of the benefits of public-private partnerships to build more robust cyber resiliency for businesses, institutions and individuals.

"The government has a very broad view of national security threats to critical infrastructure and lines of sight that the private sector doesn't have," Bailey said. "Conversely, the private sector may have intelligence on a string of malware or some other vulnerability through direct experience that the government may not have. By building bridges between the public and private sectors for the sharing of intelligence, we can leverage that information to enable greater cyber resilience for all parties."

Partnerships between risk engineering and cyber security teams within Bailey's own organization are also seeking ways to frame Zurich's cyber risk insights for the benefit of customers.

"We are actually beginning to leverage a lot of the information that our own internal security team develops for us in ways that can ultimately help customers," Bailey said. "Case in point, our business units often receive alerts from our internal Information Security team about a new cyber threat or vulnerability that has been identified in the external marketplace. The alerts tell us what's out there, what we know about it, and some of the things we can do to protect against it. It's great information – so good, in fact, that we sat down with our IS team and asked why we couldn't share this information with our customers, similar to the way we share warnings about oncoming hurricanes. We are exploring ways to share this information with customers whenever the opportunity may arise. And that's just the beginning. There are other services, including security awareness training, where our cyber risk engineering is going to play a crucial role in helping our customers and their employees develop a mindset of resilience against cyber risks."

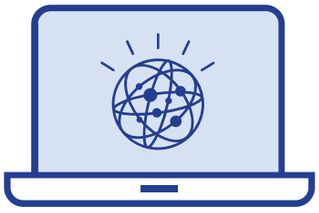
Bailey noted that building effective cyber risk preparedness and resilience strategies means looking at all the angles – not just the impact of a direct attack on a single organization but also the downstream consequences of an attack on entities the organization depends upon to sustain business operations.

"Risk managers need to think beyond their own four walls – not just within their own organizations now," Bailey said. "It's not enough to only focus on your own company and what you can do from a cybersecurity standpoint anymore. You have to be thinking about how a major attack on another entity, or even critical infrastructure, might have an impact on your business."

"It's not enough to only focus on your own company and what you can do from a cybersecurity standpoint anymore. You have to be thinking about how a major attack on another entity, or even critical infrastructure, might have an impact on your business."

[1] "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)." Statista. 2018.

ZURICH®



THE RISKS AND REWARDS OF

CYBER INNOVATION

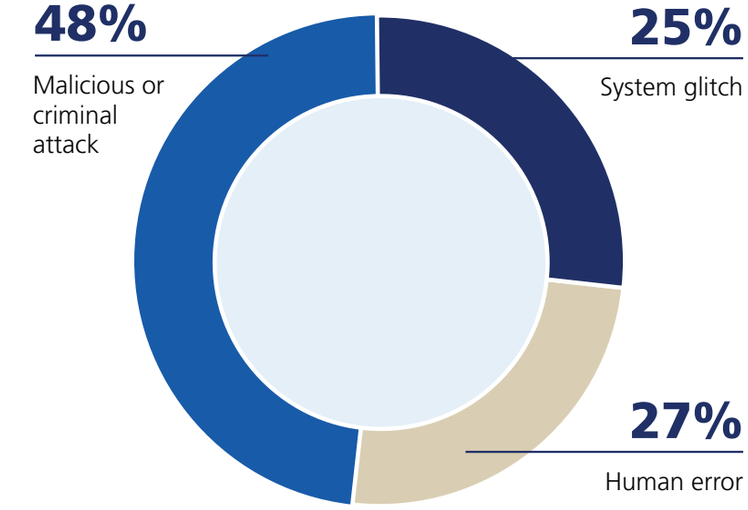
To succeed in meeting and exceeding changing customer expectations in our digital environment, organizations must deploy and leverage exciting new innovations. But inevitably, new technologies, processes and approaches bring new risks, especially those vulnerable to cyber risk.

INDUSTRIES WITH THE HIGHEST PER CAPITA BREACH COSTS (MILLIONS)[1]

HEALTHCARE	FINANCIAL	SERVICES	PHARMACEUTICALS	TECHNOLOGY
$408	$208	$181	$174	$170

$3.86 MILLION Average total cost of a data breach (all segments).[1]

ROOT CAUSES OF DATA BREACHES[1]



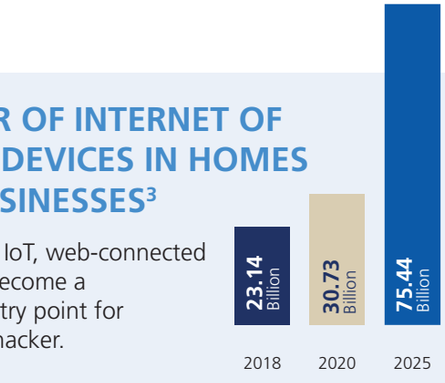
$53 BILLION
Potential global estimated in extreme, "worst-case" cloud service disruption.

Equivalent to property losses from a category 5 hurricane.[2]

19% - 250%
Potential global increase to insurance industry loss ratios due to a large-to-extreme loss.[2]

NUMBER OF INTERNET OF THINGS DEVICES IN HOMES AND BUSINESSES[3]

Virtually any IoT, web-connected device can become a backdoor entry point for a malicious hacker.



For more information about cyber risk and the emerging challenges of our connected world, visit the Zurich Knowledge Hub at zurichna.com.

1. 2018 Cost of a Data Breach Study: Global Overview, Ponemon Institute LLC and IBM Corporation.
2. Counting the Cost – Cyber exposure decoded, Cyence and Lloyd's of London.
3. Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions).

Predictive analytics tools and innovations are transforming insights into impact

Since the beginning, data has been the foundation upon which the insurance industry was built. The ability to analyze data enables the industry's capacity to effectively assess customers' risks and respond appropriately when losses occur. But at a time when a literal deluge of data is coming from all directions, the challenge facing data-driven industries – including insurance – is finding ways to analyze exponentially growing bodies of information for insights to enable better decisions, drive innovation and sharpen perspectives about the road ahead.

The adoption of cutting-edge predictive analytics, powered by such tools as artificial intelligence, cognitive computing and smart algorithms, is transforming the ability to anticipate changing customer needs. A heightened ability to predict and respond to change can become a powerful differentiator within an economic, geopolitical and marketplace environment in constant flux.

"Our customers are dealing with an evolving landscape of risks and rising costs and need our support," said **Peter Hahn**, head of Predictive Analytics, Zurich North America. "We believe we can provide that support to help them to not only better understand and manage risk using the predictive analytics tools at our disposal, but to also mitigate those risks early on in the claims process. We're really trying to transform insights into impact for our customers and distributors, helping them drive to positive outcomes."

Zurich's predictive analytics approach generates insights from a global base of proprietary and external aggregated data to identify future risks and improve decision-making. Extensive modeling capabilities augmented by new and emerging data management technologies help Zurich specialists better understand customer risks both locally and globally, information that can be shared with customers and brokers.

Putting analytics to work for customers

"Our predictive analytics methodologies are aimed at providing a deeper and broader analysis of hard-to-predict events, focusing on loss events of generally low frequency, but with the potential for high severity," Hahn said. "Using our own claims data and data from external sources we can develop models that can help us predict the course that even a single claim is likely to take. For example, after a property claim is submitted, we will run it through our models to identify if they are also at risk of a severe business interruption. This enables us to support our customers earlier with actions to mitigate the duration of interruption and reduce cost drivers of the claim."

Hahn noted that Zurich's historical research on workers' compensation claims demonstrated that when a claim is identified as benefitting from a nurse case manager, early nurse intervention within the first 30 days of the claim can save as much as $6,000-$26,000 per claim, with nearly 50 percent of that savings in medical spend.

"Using the predictive analytics tools we have, we are able to make predictions about whether an injured worker can benefit from the services of a nurse case manager two and a half times faster than in the past," Hahn said. "That leads to a much better outcome, not only on the financial side but also the 'people side.' There are some truly inspirational examples of nurse case managers playing an instrumental role in helping injured workers return to their jobs and normal lives more quickly. We can help connect our nurse case managers with the injured workers who will benefit the most. That's what I find inspiring and exciting about the promise of predictive analytics."

Predictive analytics tools are also quite effective in the property insurance arena, helping underwriters and risk managers assess the increasingly costly impacts of worsening floods around the world and their impacts on customers.

"We have some very effective models that look at flood risk," Hahn said. "We strongly believe that part of our service to customers is being able to quantify and assess the risks they face to help make more informed choices about where to site a building and how to mitigate the risks of existing buildings that could be hit by floods."

Hahn expressed genuine excitement about the prospects for evolution and enhancement of predictive analytics tools in the years to come.

"We are continuously excited about what's ahead," Hahn said. "We see many opportunities to continue to grow the impacts and benefits of predictive analytics for our company, our customers and our distribution partners. I have no doubt whatsoever that the opportunities presented by artificial intelligence, cognitive computing and other tools will continue to expand. This is a very exciting time for this discipline at Zurich and at many other companies."

"Our predictive analytics methodologies are aimed at providing a deeper and broader analysis of hard-to-predict events, focusing on loss events of generally low frequency, but with the potential for high severity."