BEST'S REVIEW
www.bestreview.com July 2019

Technology

Fight Fire With Fire

Digital data is creating a cyberrisk. Digital products and processes must have security measures built in from conception to ward off cyberattacks.

Our world is becoming more digital. Businesses are becoming smarter, more efficient and more responsive and consequently cyberrisk is growing, too.

Digital technologies and data are being used across the value chain. Analytics and automation are being embedded into our business processes and at the same time contract labor and remote employees are being used. We are exchanging more data with customers, producers, solution providers, suppliers and other business partners. This is both good and bad. While it's good for productivity, it's bad for cyberrisk. Increasing amounts of data, use of connectivity and automation multiplies the opportunities for cyberattacks.

A cyberattack occurs every 40 seconds, totaling approximately 750 million attacks annually. Both data and programs can be hacked. Algorithms can create tainted output. Hacking a robot, drone or autonomous vehicle can cause injury or even death. Breaches of customer data can destroy customer trust and even a company's reputation and stock price.

This creates risk for us as individual companies but also creates opportunities for us as an industry to insure and mitigate cyberrisk.

The problem is that the risk is so pervasive and ever-changing that our time-tested approach of using past losses to predict future ones falls short. First, we simply do not have enough credible data—not just volumes of information, but years of data. Second, we can't foresee the types of events that have not yet happened. Much like fraudsters' ingenuity, hackers' creativity is boundless.

Risk prevention and mitigation processes can help manage and reduce loss frequency. Progress is being made. Last year only one in eight focused attacks penetrated network defenses, compared to one in three in the prior year, according to Accenture's *State of Cyber Resilience* report.

By
Pat Saporito

Risk is so pervasive and ever-changing that our time-tested approach of using past losses to predict future ones falls short.

Current approaches will likely not be enough for the future. Today's security efforts are largely focused on detecting and deflecting damage to core corporate IT systems and data. Digital products and processes need to be made safer in their design and by engaging business leaders as well as employees during development. Data governance and security should be part of all employee onboarding. A "security first" culture should be developed not only with employees but also with partners and suppliers.

While cyber liability is underwritten just once a year, cyberattacks are continuous. As underwriters, we can mandate continuous risk management efforts. We could mandate risk assessments not only as part of the initial underwriting process but as a condition of continuous coverage. These can include compliance checks against standards such as the National Institute of Standards and Technology cybersecurity framework or regulations such as the EU General Data Protection Regulation, the Payment Card Industry Data Security Standard and the Health Insurance Portability and Accountability Act.

We can also fight fire with fire and use technologies like artificial intelligence to deploy algorithms against information in corporate systems and data stores.

It's imperative to develop a collaborative effort with policyholders and not merely invoke a defense posture on cyber. We can require these efforts much as we do safety procedures for workers' compensation insurance.

We will become better underwriters of cyberrisk as we become better cyberrisk managers of our own risk. Underwriter, underwrite thyself! BR

Best's Review columnist **Pat Saporito** is a partner at Digital Business Creations LLC and author of *Applied Insurance Analytics: A Framework for Driving More Value From Data Assets, Technologies and Tools.* She can be reached at *pat.saporito@suretywave.com.*