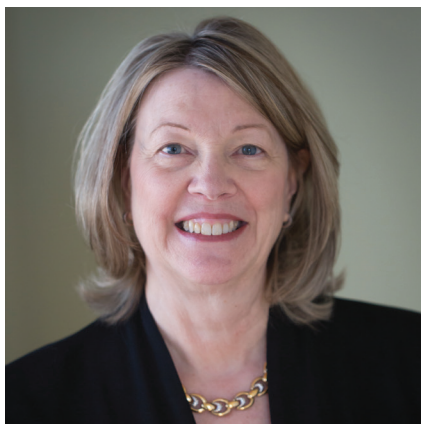
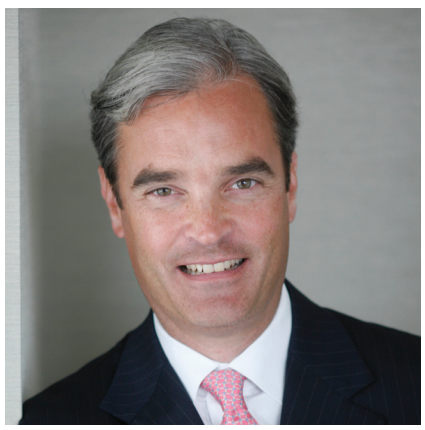
Team effort needed to tackle expanding cyber threats





Laura Foggan is a partner in Crowell & Moring L.L.P.'s Washington office, where she is a member of the firm's insurance/reinsurance group. She can be reached at lfoggan@crowell.com and 202-624-2774.

Jack Thomas is the managing partner of Crowell & Moring L.L.P.'s London office. He is a member of the litigation, insurance/reinsurance and international dispute resolution groups. He can be reached at jnthomas@crowell.com, 44-20-7413-0011 and 212-895-4306.

Annually, more than half of U.S. businesses experience cyber attacks. With attacks increasing, insurers have refined and expanded their policies, but as they do so they must take care to develop policies that best respond to complex and evolving threats. Doing so will allow insurers to increase their market share and profitability, protect their policyholders from nefarious actors and untoward events and, ultimately, benefit society.

The severity of cyber attacks is also increasing. The average size of a data breach has surpassed more than 24,000 records, and estimated annual losses from cyber crime now top $400 billion. The potential harm from accidental cyber incidents also has skyrocketed as technology becomes embedded in every aspect of what we do.

The most activity in the cyber insurance field is seen in the increasingly robust and competitive specialty insurance market, which has developed stand-alone products that provide deeper and more complex coverage. Gone are the days when coverage was limited to breach notification costs, call center offerings and forensic or crisis management services. In this competitive marketplace, insurers seek to differentiate themselves by identifying added value that can be built into their programs to meet unaddressed cyber-related needs. For instance, many in the market are discussing the possibility of coverage to address the financial impact of cyber events on an organization's reputation.

At the same time, cyber insurance buyers often don't understand their exposures and the type of coverage they need, especially as cyber risks frequently change. Insurers need to explain and quantify exposures to their policyholders and mitigate their own risk by delineating where their coverage begins and ends. An insurer may be prepared to cover a cyber incident arising from one employee's mistakes, for example, but not willing to take on a company's losses when a whole department fails to adhere to appropriate cyber hygiene standards.

Insurers can provide incentives for good cyber security practices by placing some of the burden on the policyholder. Some have taken steps to do so, including policy language that requires policyholders to meet and maintain certain information security management guidelines and practices such as following recommendations for updating software and maintaining vigorous malware screens. Policyholders who fail to meet the best practices standards for computer security may forfeit their insurance coverage.

Others offer discounts for companies that have programs for vulnerability disclosure, such as voluntary "hack" events designed to help discover vulnerabilities in digital platforms, products and information technology systems. And others include a stipend toward cyber awareness and prevention training as part of their coverage package.

As cyber coverage continues to evolve, insurers are wrestling with ways to measure more precisely the sophistication of a company's cyber risk management. Many are underwriting based on third-party assessments confirming the level of cyber risk, rather than using questionnaires. And insurers are forming alliances with other businesses, to offer enhanced cyber insurance options paired with cyber resilience evaluations, secure technology and incident response services.

The challenge all cyber underwriters face is a lack of underwriting data and an uncertain legal landscape for cyber liability. Underwriters traditionally rely on years of data to write policies, but cyber losses and liabilities are still evolving. For example, a spate of recent ransomware breaches shifted the cyber threat for many entities from costs associated with responding to criminal or inadvertent disclosure of private information to harm arising from ransomware attacks blocking access to systems or records and interrupting business.

The challenge all cyber underwriters face is a lack of data and an uncertain legal landscape for cyber liability ... cyber losses and liabilities are still evolving.

When pharmaceutical giant Merck & Co. Inc. was hit by the NotPetya ransomware attack in June 2017, hard drives on its computers were encrypted so that the machines could not run. This disrupted production of some of Merck's medicines and vaccines. The attack may have cost the firm more than $300 million in the third quarter of 2017 alone, according to the company.

WannaCry, which last year targeted computers running Microsoft Windows by encrypting data and demanding ransom payments in bitcoin, affected major hospital systems, shutting down medical equipment and blocking practitioners from accessing patient records. Insurers evaluating such scenarios must consider a wide range of consequences, including exposure to business interruption and medical malpractice losses.

One of the most vexing questions is determining how insurance should respond to cyber physical risks, i.e., loss from a hack or disruption of a cyber system that may result in physical harm — bodily injury or property damage. To date, specialty cyber coverages have almost exclusively focused on intangible assets and generally have not included coverage for physical losses. This may change as there is increased recognition of the bodily injury and property damage exposures that are possible in the event of a hack of electronic industrial control systems, or "smart" devices that make up the "internet of things." Although refining stand-alone cyber insurance products is one option to address cyber-physical risk, there also has been some movement to incorporate cyber-physical risks into traditional lines of coverage, such as property insurance.

A few insurers have announced intentions to cover physical damage resulting from cyber incidents under property coverage, generally with a designated sublimit. Insurers offering traditional property coverages have the institutional knowledge to measure and respond to large-scale property losses, such as a fire destroying a factory because of a hijacked industrial control system. Property insurers' expertise in valuation of the loss of a physical plant, for example, as well as business interruption issues from the shutdown of factory operations, may position them to better assess damage in these scenarios.

Property underwriters may need to develop specific expertise to assess cyber risks, as measuring damages and assessing vulnerability are two different things. Valuating an inventory loss is not the same as projecting the likelihood of a major loss from a software defect in a "smart" commercial refrigeration unit, or the likelihood that cyber criminals will disrupt electricity necessary to a manufacturing plant.

It is difficult to predict whether certain cyber risks — particularly cyber-physical risks — ultimately will reside principally in stand-alone cyber policies or be incorporated into traditional property/casualty policies. It is possible, and even likely, that both approaches will continue to thrive for the foreseeable future. The best "fit" for cyber risk will depend on two key considerations: the nature of the potential losses for which coverage is sought and the scope of the coverage options available under traditional lines and specialty stand-alone policies.

When it comes to protecting society from cyber risk, everyone has a role to play: Insurers increase resilience by educating businesses on how to avoid risk and helping to finance a response if a cyber attack occurs; policyholders need to do their part to identify, implement and monitor effective cyber security standards; and government has a role to play in promoting policies that will minimize cyber risk and enhance resiliency, including by treating insurance as an essential weapon to tackle cyber crime and other potential cyber loss.