# Evolving Coverage for Cyber Exposures

*By: Colby Hewitt, CPCU, AIAF, ARe*

Cyber security can be a frightening and confusing topic. The news bombards us with reports of hackers and gangs disrupting oil pipelines, infiltrating web services companies and stealing private data from massive chain stores. Horror stories abound regarding attacks to all scale and manner of businesses and individuals.

We see with increasing clarity that, no matter how large and savvy or small and innocuous, every person and business is exposed to cyber hazards. Furthermore, individuals working from home may be at greater risk of compromise.

With awareness comes demand, with demand a market opportunity, and with that opportunity a responsibility to provide solutions to policyholders.

A myriad of cyber products exists in the current market, addressing both personal lines and commercial lines exposures. These products usually provide monetary coverage for financial loss and costs associated with recovery. Coverage may also include access to professional recovery services.

Coverages and pricing can vary dramatically, and specific coverages, of course, depend upon the form. Carriers and agents alike should be versed on the spectrum of available coverages and the exposures against which they protect.

## Cyber Attack

When an attack occurs, the damage to the victim's system and data, as well as the compromise of information held in that system, are immediate concerns.

A cyber attack comprises any unauthorized access of a computing device or the receipt of code by such a device that destroys or alters data. As a result of a cyber attack, the victim may suffer a first-party loss, including damage to their system or files, incurring data recovery and system restoration costs.

In addition to a victim's own first-party loss, a cyber attack could result in the victim passing on malware to a third party, which could result in additional third-party liability exposure. Expertise may be necessary to identify the scope of damage and the best means of recovery.

Data response services are necessary when a cyber attack results in the compromise of personally identifiable non-public information held by the victim; this can include their own data or data held on behalf of other people. Coverage may also be triggered when paper or electronic files are compromised due to an accident or negligence by the policyholder. Both breach notice law and general goodwill dictate that notification to affected individuals is necessary in these instances. Cyber policies may provide call center, public relations and crisis management services such as credit monitoring to handle the impact. Coverage may also be afforded for defense, fines and expenses resulting from such information being compromised in a cyber attack.

## Cyber Extortion & Social Engineering

In addition to the actual stolen information, hackers utilize ransomware and the threat of damage and data compromise to extort payments from victims.

Cyber extortion involves a demand for funds to prevent a cyber attack or related to an ongoing cyber attack. The victim may be locked out of their system, and private information of theirs or others may be threatened until a payment is received by the parties behind the hack.

Social engineering fraud occurs when a threat received over digital communication, credible or not, results in the transfer of funds to a fraudster. While cyber extortion involves a credible or ongoing threat, social engineering relies on psychological manipulation. Coverage for social engineering varies widely and may be dependent on how the funds are sent (i.e., whether they are traceable). In some cases, the coverage provider must be notified before funds are transferred if coverage is to be afforded.

In the case of both cyber extortion and social engineering, law enforcement may need to be involved for coverage to trigger.

## Named Viruses

It is worth noting that some, but not all, coverage forms exclude named viruses. A named virus, such as WannaCry, CryptoLocker and ILOVEYOU, presents a catastrophic exposure that can cause tens of millions of dollars in damage. Forms that exclude named virus do so in part because these viruses may be of a relatively modest cost to the victim, but with a massive aggregate impact.

## Cyber Bullying

Financial loss and liability are certainly frightening, but few concepts are more pervasively terrifying, especially to a parent, than cyber bullying.

Cyber bullying is harassment or intimidation, usually recurring, that is committed over a computing device and results in mental anguish. Some personal lines forms may provide coverage for relocation, mental health services, tutoring and increased cost of education incurred as a result of a cyber bullying incident.

## Conclusion

Policyholders that buy cyber insurance coverage in its many forms should be apprised of the extent of the coverage they are purchasing and duties they may have in the event of a loss. Such duties may include, but are not limited to, timely reporting and the involvement of law enforcement. Some may also require preventative safeguards.

As these exposures evolve, so too will the options for covering them. Cyber insurance will continue to be one important weapon in the defense of these emerging risks, and an educated insurance professional can add value for the consumer by better understanding these products. ■

*Colby Hewitt, CPCU, AIAF, ARe, is chief marketing officer for The Norfolk & Dedham Group, providing complete insurance solutions through independent agents since 1825.*