THOMSON REUTERS

Westlaw®

Cyberattacks: Is your firm protected?

By Renata L. Hoddinott, Esq., and Howard M. Garfield, Esq., *Haight Brown & Bonesteel*

AUGUST 25, 2017

Thousands of companies throughout the world are still recovering from the worldwide ransomware attack that struck about 300,000 machines in 150 countries May 12.

The WannaCry ransomware sequestered the data on each infected machine, holding the information hostage and demanding payment of a ransom for release. The amount of the ransom increased the longer the user took to pay.

The ransomware targeted business, individuals and even the U.K.'s National Health Service.

Within the first few hours, desperate users anxious to recover their data and regain the use of their computers paid thousands of dollars (in bitcoins) in ransom.

Viruses and ransomware are not new. However, they may have grown in size and strength. They attack without warning and regularly demonstrate they are here to stay.

News stories are replete with examples of the cyberthreats that companies now face.

In the past few years, retailers Saks Fifth Avenue, Home Depot and Target have all been attacked. These attacks compromised the financial data of customers and created a public relations nightmare.

In 2015 hackers targeted UCLA Medical Center and accessed parts of the hospital's computer network containing patients' personal and medical information.

UCLA had to hire private computer forensic experts to secure information on its network servers. It also provided free identity protection services to patients who were potentially affected by the attack.

As yet another example, several recent news stories involve intrepid thieves who equip ATM machines with "skimming" devices that they simply slip over the machines' card readers.

When customers insert their cards into the machines, the skimmers read and copy all the information from the cards, allowing thieves to create and use fraudulent copies.

Though the devices do not damage the machines, they wreak havoc and cost banks thousands of dollars in reimbursements to defrauded clients.

Although banking institutions face significant risks due to these skimming schemes, traditional insurance policies may not cover losses relating to ATM "hacks." Traditional policies may provide coverage only for "smash and grab" attacks to ATMs or other incidents involving physical property damage.

Despite the recent onslaught of cyberattacks, many businesses and firms leave themselves vulnerable by falsely believing they have insurance to cover the damage these attacks inflict.

Although banking institutions face significant risks due to skimming schemes, traditional insurance policies may not cover losses relating to ATM "hacks."

Of course, there are many different kinds of insurance coverages available to businesses and firms. Most companies have a commercial general liability or business owner policy and add specific endorsements for other protection they might need, such as coverage for business interruption or employee dishonesty.

However, companies now face significant risk from unseen threats such as viruses, hacking and other data breaches, which typical business policies do not cover.

Cyberattacks present two major data-related risks against which most businesses mistakenly think they are insured.

The first is a risk of loss to the property of the business or professional, resulting in compromised operations and business interruptions as well as loss of revenue.

The second risk of loss relates to privacy interests in compromised sensitive financial or personal information that belongs to a business's customers or clients.

PROPERTY DAMAGE AND CYBERCLAIMS

Unfortunately, most traditional business property policies cover only "direct physical damage" to covered property, such as when lightning causes an electrical surge that destroys hard drives.

Moreover, many property policies expressly provide that "data" are not "covered property." In other words, businesses may find themselves without coverage for loss of data if there was no physical damage to the hard drive and they did not add an endorsement or other type of patch to the policy.

REUTERS/Graphic

Most companies with traditional business property policies are not insured against cyberattacks such as WannaCry, the worldwide ransomware attack that affected 300,000 machines. A WannaCry ransom demand is shown here.

While some viruses corrupt data, others simply erase information. Still others alter access codes and hold data hostage until a ransom is paid, such as in the recent WannaCry attack.

Further, when an entity suffers a ransomware attack or any cyberattack, even after information is recovered or access to data is resolved, common practice dictates replacing the affected hardware.

This is because it is virtually impossible for an information technology department or internet security consultant to guarantee that a machine that has suffered a cyberattack is completely "clean."

There is always a risk that the virus or malware left behind some remnants or "sleeper cell" that lurk in the background and can be awakened by command to cause further chaos and damage.

Unfortunately, traditional policies do not cover the cost of replacing machinery when that is the case. They provide coverage for risk and resulting damages — and not for prophylactic measures where no damage has yet occurred.

Policy patches that add virus coverage to a traditional business property policy are frequently inconsistent with the language of the body of the policy, and they also may not provide sufficient protection.

Depending on the specific attack and the definitions set forth in the specific policy, damages resulting from a cyberattack or malware may not be covered even with some endorsements.

COVERAGE FOR PRIVACY LAWSUITS

Lately, the insurance industry has done a better job of catching up with providing liability solutions for professionals or businesses that have suffered a data breach that compromises their clients' or customers' privacy rights.

Aside from protection against privacy lawsuits, these policies should reimburse the insured for the usual costs of providing credit monitoring and the like to clients or customers. However, there is much room for improvement with respect to both risk analysis and coverage underwriting in this area.

If recent events have taught us anything, it is that cyberthreats are very real and can affect a broad range of industries.

In fact, almost any professional or business faces the risk of significant damage from a cyberattack.

Given that every company — ranging from accounting firms, law firms and healthcare facilities to large corporations and even "mom and pop" stores — has unique exposure to these unseen threats, it is imperative for businesses and firms to identify their specific potential vulnerabilities and work with their IT professionals, brokers and insurers to close the risk gap.

For some, crafting a unique policy may be the right decision in the long run.

This need for technical awareness also flows to insurance companies' brokers and underwriting teams, whose clients will ask for this type of coverage.

There could also be potential exposure for brokers who fail to properly assess the risk facing their clients and ensure the correct type or amount of coverage necessary for that specific business.

PROACTIVE MEASURES

To ensure your or your business's security, you should implement the following measures.

Conduct a cyberthreat assessment

A small business or professional firm that does not have an IT team or cybersavvy employee will need the services of an IT consultant who is knowledgeable about the ever-changing world of cyberthreats.

> Despite the recent onslaught of cyberattacks, many businesses and firms leave themselves vulnerable by falsely believing they have insurance to cover the damage these attacks inflict.

Companies that professionally assess these risks are springing up everywhere. In the future, every brokerage that purports to help its customers find the right kind of cyberinsurance will need a dedicated team of cyberprofessionals to help clients evaluate current and emerging risks of cyberattacks.

These professionals will need to work with each customer to identify its unique risks and understand the language of insurance either to identify the appropriate policy or to customize a policy to insure the professional or business against cyberattacks.

Secure a broker

A broker will be knowledgeable about which insurance companies have acquired some familiarity with cyber risks.

A knowledgeable broker should try to steer a client to carriers that have been underwriting cyber risks for some time.

Ideally, of course, the modern underwriting team will include the same kind of professional who assesses current and emerging cyber risks for the business.

Though cyberthreats can be intimidating, there is no need to be overwhelmed.

You don't need to be an expert — you just need to make sure you have someone on your team who is cognizant of these issues and can help you or your clients assess the risks facing your business in today's ever-changing cyberthreat world.

This article first appeared in the August 25, 2017, edition of Westlaw Journal Computer & Internet.

ABOUT THE AUTHORS


Renata L. Hoddinott (L) is an associate in the San Francisco office of **Haight Brown & Bonesteel**. **Howard M. Garfield** (R) is of counsel in the firm's San Francisco office. Both attorneys are members of the firm's professional liability practice group and risk management and insurance law practice group. They can be reached at rhoddinott@hbblaw.com and hgarfield@hbblaw.com, respectively.