METROPOLITAN
CORPORATE
COUNSEL®

OCTOBER 2017 WWW.METROCORPCOUNSEL.COM

SPECIAL SECTION: CYBERSECURITY

This Is No Time to Stand Pat

As cyber threats morph, companies need to reassess their readiness, including their insurance protection

By Joshua Gold / Anderson Kill

In the present environment, cyber risk management simply cannot stay static. Cyber risks continue to morph and vex organizations worldwide. Recent incidents represent a cross-section of nightmare scenarios for businesses, governments and others. They included a large insurance company's $115 million patient breach settlement; an SEC breach investigation preceding a reported $350 million (downward) price adjustment for a corporate acquisition; an $81 million cybertheft from what was thought to be perhaps the safest banking network on the planet; the sudden shutdown of UK hospital networks; law firms losing control of privileged client files; theft of yet unreleased films and original cable programming; and the destruction of industrial facilities in Europe and Asia.

Cyber Risk Management Has Never Been More Important

To have even a fighting chance against the threat of security incidents, every organization must put in place a proactive and comprehensive cyber risk-management plan. Below are several steps organizations can take to improve their cybersecurity resilience. While certainly not an exhaustive list, these four actions can prevent many security breaches and minimize the impact when these types of intrustions hit your organization.

1. Map and safeguard data: It is difficult to draw up a game plan to protect data if you don't know what you have and where it is. Mapping may yield some surprises – revealing, for example, that divisions or individual employees use their own cloud computing, whether company policy permits such hosting or not. Thus, organizations need to map all data for which they are responsible. Additionally, because so many organizations use some form of cloud computing these days, data not on your own servers needs to be accounted for, since you can anticipate that a regulator will deem you responsible for it no matter whose server it resides on. There have now been several high-profile hacks where the criminal attacked the organization through information residing on another entity's computer systems.

2. Update and patch: Malware attacks carried out by WannaCry, GoldenEye and NotPetya are believed to have exploited those computer systems that had not updated their system security to apply software manufacturer patches. Basic hygiene is required when it comes to making sure that programs are updated regularly – especially where those updates are motivated by security concerns. Many hackers target the low-hanging fruit.

3. Keep senior management involved: Gone are the days when senior management could relegate cybersecurity oversight to the head of IT. A sufficient dedication of money, human resources and direct senior manager involvement is required – especially if the organization is a public company. The Securities and Exchange Commission has made it clear that it will investigate the disclosure and handling of cybersecurity incidents, and it has already flexed its regulatory muscle, fining a broker-dealer who was alleged to have failed to adequately protect customer data. Many companies have prudently created the senior officer position

ANDERSON KILL
ATTORNEYS AND COUNSELORS AT LAW

of chief information security officer (CISO) and provided that position with access to the highest management levels of the organization.

4. Disclose risks and incidents: Smart risk management requires accurate disclosure of the risks faced and the cybersecurity efforts of the organization. The SEC has provided guidance to public companies on the types of computer system assessments that should be taken into consideration. The FTC has vigorously pursued companies that it says failed to accurately describe their cybersecurity wherewithal. If a breach takes place, prompt disclosure, barring law enforcement instructions to the contrary, is the prudent course. Some regulators and law enforcement officials (both state and federal) expressly say that it is an automatic red flag if policyholders do not disclose a cyberbreach within 30 days of its occurrence.

Insurance as a Key Risk-Management Tool

If a policyholder suffers a cyber-related loss, it may certainly have coverage under a specialty cyber insurance policy. Often, however, the analysis does not stop there. A policyholder may also find insurance coverage for a cyber claim under directors and officers (D&O) insurance, errors and omissions (E&O) insurance, property insurance, crime insurance and commercial general liability (CGL) insurance. If a cyber incident takes place, policyholders should promptly notify all potentially applicable insurance policies.

Don't Be Misled by Titles

The purchase of specialty cyber insurance products is on the rise, and the insurance products geared specifically toward these perils have evolved considerably. Despite this, figuring out what kind of insurance is needed to respond effectively to cyber claims is challenging. Just because an insurance policy contains the word "cyber" in the policy description does not mean that the insurance company will be willing to pay a related claim. For example, a recent decision from a federal court in Utah ruled that a CyberFirst liability insurance policy did not cover a claim involving alleged wrongful acts in the handling of data. (*Travelers Property & Cas. Co. v. Fed. Recovery Serv., Inc.*)

Recent history teaches us that court decisions can be all over the place on similar issues. This year, two policyholders seeking "computer fraud" coverage under their crime policies fared quite differently. In *American Tooling Center Inc. v. Travelers Casualty and Surety Co. of America*, a federal trial court in Michigan held that there was no coverage for wire transfers made when the policyholder was duped by fake emails into wiring money to a bogus bank account. The trial court held that there "was no infiltration or 'hacking' of [the] computer system," and that the "emails themselves did not directly cause the transfer of funds; rather, [the policyholder] authorized the transfer based upon the information received in the emails." Conversely, a federal trial court in New York found computer fraud coverage, among other things, for wire transfers that the policyholder was induced to make through fraudulent emails and follow-up phone calls. (*Medidata Solutions v. Federal Ins. Co.*)

Court rulings have also differed on the extent of insurance protection for cyber class-action privacy claims under general liability insurance. In coverage litigation, a New York trial court held the policyholder had no CGL insurance coverage for privacy litigation stemming from a hack of customer information located on the servers of a multi-tenant cloud platform. (*Zurich American Ins. Co., et al v. Sony Corp. of America*) The case was settled before a New York appellate court ruled on the policyholder's appeal.

Last year, however, the United States Court of Appeals for the Fourth Circuit held that a CGL policy covered privacy litigation defense costs for patient medical information that was left on a publicly accessible searchable server. (*Travelers Indemnity Co. of America v. Portal Healthcare Solutions LLC*)

Here are a few additional issues you may wish to work out with your underwriters at the time you purchase a policy rather than after you file a claim.

Exclusions for terrorism, hostilities and warfare: New revelations have emerged that many attacks come from state-sponsored hacking gangs. Some U.S. lawmakers have described such activities as cyberwarfare. In light of this, policyholders should work with their brokers to get clarification regarding the scope of terrorism and war risk exclusions. For example, many cyber insurance policies contain exclusions for terrorism, "hostilities (whether war is declared or not)" and claims arising from "acts of foreign enemies." Experienced brokers can work to get the most favorable language for policyholders in this area.

Be careful with your board's D&O insurance: It is important to make sure that D&O insurance coverage (including primary, excess, Side A, etc.) remains free of cyber-related exclusions or sublimits. Management will be highly concerned with any argued "gap" in coverage, should a cyber event ensue – especially with the advent of cyber derivative shareholder litigation. Home Depot recently settled derivative litigation aimed at its senior management, and the SEC has repeatedly made clear that it will enforce cybersecurity compliance matters against the entities under its purview.

Cover time-element losses: Business income coverage and reputational damage coverage take on added importance in the wake of recent hacking events designed to harm, destroy and kill. Cybercriminals now have the means to reach industrial controls, attack transportation and other infrastructure, and cause explosions by remote control. As such, business interruption takes on greater importance for policyholders that are industrial or critical infrastructure targets.

Avoid reasonableness representations and clauses: Policyholders should work with their brokers to avoid exclusions, warranties, representations or "conditions" in insurance policies concerning the soundness or reasonableness of the policyholder's data security efforts/protocol. These clauses are a recipe for disputes on potentially every security incident.

Cyber coverage litigation has already emerged involving a cyber insurance company's allegations that the policyholder failed to employ computer security measures it had represented would be in place. (*Columbia Casualty Co. v. Cottage Health System*) Given the pace of technological innovation, almost every computer security step can be second-guessed. Many insurance companies will now forgo these clauses – if requested.

Cover cloud and third-party vendors: Make sure that your specific cyber coverage protects against losses where others manage, transmit or host data for your company. Insurance coverage is available for cloud computing and instances where data is handled, managed or outsourced to a third party. Most cyber policies can be modified to extend needed protection to data residing on servers not owned by the policyholder – if requested.

The Bottom Line

There is no single step that will guard against cyber risks. The protection against these risks and the risk transfer to address

potential losses are properly viewed as a process. While no one is immune from cyber threats (and no one expects anyone to be impregnable to such risks), investors, customers, regulators and other stakeholders will expect that organizations take the risks seriously and dedicate sufficient resources to reducing the threat of an intrusion, and that they have a plan in place to stem the harm if a hacker gets through.

Joshua Gold *is a shareholder at Anderson Kill in New York and is chair of the firm's cyber insurance recovery group. He regularly represents policyholders in insurance coverage matters and disputes concerning electronic data, arbitration, time element insurance and other property/casualty insurance coverage issues. He can be reached at jgold@andersonkill.com.*