FINE PRINT

Risk Management for "Hacker-less" Security Risks

by Joshua Gold

Criminal cyber gangs, hackers and internal employee theft threats are understandably the focus of risk managers seeking to address online perils. After all, international banking funds have been stolen with a few keystrokes, hackers have managed to blow up a pipeline, and election systems across the globe are targeted with growing frequency by a host of shadowy figures with unsettling resources, including foreign government backing. This year, cybersecurity spending

is expected to rise across the board for many companies, spanning various industries. The bulk of this spending is expected to be focused on thwarting the growing scourge of malware attacks. But malware, funds theft, data hacks and disruption attacks do not comprise the full spectrum of online risks. Today, many cyberrisks are of the less exotic variety and do not necessarily implicate the presence of a criminal. Liability often involves pedestrian errors, software glitches, and inattention to handling data safely. Such inattention can violate the law under new regulatory schemes.

DATA PROTECTION LIABILITY

Lawmakers and regulators are increasingly mandating that sound protocols be followed concerning the collection, hosting and transmission of data. The well-publicized GDPR and California's enactment of the CCPA epitomize efforts to put consumers, patients and online users in a position of data privacy, data safety and data control. Twice last year, GDPR fines in the nine figures were sought against international companies based upon inadequate security procedures that allowed access and misuse to data. But unauthorized access is not the only potential regulatory exposure. Another international tech company was fined for non-GDPR compliant data "processing" transparency, including a lack of clear and easy to read disclosure over data storage periods and the use of personal data for commercial online business. Notably, no breach was alleged in that instance. The CCPA mandates a "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information" and various fines and liability exposures may arise under California's (recently implemented) analog to the GDPR.

Online actions have to comport with safety, disclosure and privacy considerations of the individual whose data is in the hands of others. While liability can arise for failing to secure individual data from a hacker, it can also arise in the absence of any hacking event. It may be enough, for example, that sensitive data is placed on a server that is susceptible to an online search.

Several cases over the past few years have underscored the risk of mishandling data—even where no crime and no criminal are evident. In one class action, patients whose private medical data was exposed on servers that could be searched on the internet commenced a privacy suit. When the policyholder sought liability insurance coverage the insurance company denied the claim, leading to yet another lawsuit to address the scope of insurance protection for privacy class actions. The federal appeals court held that the insurance company was obligated to cover defense of the patients' suit against the policyholder, as the information was "published"—even though there was no allegation that anyone actually accessed the patients' private medical information, let alone misused it to commit some type of wrongful act.

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com

There have been several other cases in which policyholders were pursued legally over the disclosure (or loss of control) of data where no evidence existed that anyone actually accessed the data or exploited it to the individuals' disadvantage.

INSURANCE COVERAGE IMPLICATIONS

Some federal courts have loosened the rules over who may sue and when they may sue after information is disclosed. Federal appellate courts in the Sixth and Seventh Circuits (and now elsewhere) have taken a less strict view over when litigants may sue for a data breach (technically, this issue is usually referred to as Article III standing under the Constitution). Even if evidence is lacking that data has been misused to commit identity fraud or financial theft, some courts have held that class action litigation, nevertheless, can be pursued against the organization alleged to have permitted unauthorized access to private data.

Accordingly, policyholders are well-advised to make sure that they take all reasonable measures to avoid placing sensitive data in places where it can be accessed or disclosed. Whether a criminal is involved in hacking it, using it or monetizing it may not even be a factor. Rather, policyholders may have liability (including significant litigation expense and risk) where the individual's information is merely capable of being searched or accessed, irrespective of whether it actually ever gets viewed or misused.

Insurance coverage can play a key role here. Protection against liability may be available under cyber insurance products. Some cyber-specific policies will expressly cover scenarios where policyholders are liable for mishandling data or are subject to regulatory actions. Other cyber insurance products may be silent or even expressly exclude such scenarios. Policyholders are well advised to review their other insurance policy lines as well, as management liability insurance, D&O, E&O and other liability policies may offer valuable protection where data is allegedly mishandled, yet no hack or third-party bad actor is identified.

RISK MITIGATION STEPS

It is virtually impossible to be well-insulated from all cyber perils. Nonetheless, basic cyber safety measures, at a minimum, should include:

- An informed senior management, including boards of directors
- Regular employee training concerning the access, use and handling of data
- Clear (and regularly updated) data handling, use and storage procedures that are compliant with the most restrictive body of regulations that the entity is likely subject to (e.g., CCPA, GDPR, Illinois bio-metric law; New York's Part 500, etc.)
- Fair and clear disclosures over the use of data and duration of its storage
- Encryption of data on all mobile devices that can be fairly viewed as sensitive
- Regular patching and software updates for all systems
- Mapping of data within the entity to ensure that all servers are accounted for
- Smart architecture of computer systems so that if one server is compromised, the hackers are confined to that entry point
- Proper insulation of back up tapes and systems
- Detailed records of cyber security due diligence that can be used by the organization in the event procedures or unauthorized disclosures have to be explained to regulators and law enforcement. ■

Joshua Gold is a shareholder in Anderson Kill's New York office and chair of Anderson Kill's Cyber Insurance Recovery Group. He regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property/casualty insurance coverage issues.

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com