©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

Healthcare Cybersecurity

W. ANDREW H. GANTT III, EDITOR

AMERICANBARASSOCIATION
Health Law Section

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

CHAPTER 5

Risk R_x: Managing Privacy and Cybersecurity Risks

Molly McGinnis Stine and Matt Murphy

This book is for a healthcare audience that is, and must be, acutely aware of privacy and cybersecurity risks. The abundant personal and medical information aggregated by the healthcare community was among the earliest targets for threat actors and remains so today.

This chapter stresses the importance of strong risk management principles that should be revisited regularly. Each aspect of this chapter could be the focus of more detailed discussion, and perhaps this chapter will encourage even more planning and implementation. In the meantime, however, this chapter spotlights some key risk management factors.

The language around privacy and cybersecurity issues reflects a decidedly medical influence. For instance, one is encouraged to practice good security "hygiene." One worries about "viruses" attacking networks. One considers "annual check-ups." One hopes for "clean bills" of system health. To continue using healthcare vernacular, it is important to diagnose, to exercise preventive care, to seek treatment options and opinions, and to consider insurance.

I. Risk Identification (*The Diagnosis*)

A healthcare organization obtains, uses, and retains considerable information.[1] Although patient information is certainly an important component of the information that health organizations create, aggregate, and maintain, many other kinds of information exist and must be considered. Some exist because

1. Other chapters discuss some of the laws and regulations governing the information obtained or held by healthcare entities. For example, Chapter 3 ("How to Prepare for and Respond to Cybersecurity Attacks") comments on the requirement for a HIPAA security risk analysis and risk management review. In contrast, this chapter focuses on risk management issues at a more operational level, as opposed to compliance with any given legal authority.

9781634258087_Healthcare_Cybersecurity.indd 89 17/12/20 4:15 PM

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

healthcare is involved; others exist because every kind of enterprise, particularly commercial enterprises, utilizes such information. These may include:

- personal information about employees, patients, and others (name, address, date of birth, marital status, family details, Social Security numbers, and more);
- protected health information about employees, patients, and others;
- operational particulars (payroll, accounting, bookkeeping, facilities);
- business development (marketing plans, mergers and acquisitions planning);
- intellectual property (research and development, patents); and
- strategic considerations (succession planning, capital investments, hiring decisions).

In addition, much of this information may reside in your computer systems or networks and also on stand-alone computers or other devices. Some information may be web-based and available to third parties. Other information may be in folders in a file cabinet. For purposes of this chapter, we consider the information itself and the platforms in which they are stored all part of your *information assets*—all of which deserve and require appropriate privacy and cybersecurity planning and safeguards.

All of these information assets are or may be critical to you. For that reason alone, you should carefully consider taking the following actions:

- identify and inventory your information assets;
- document the location of the assets (consider both digital and hard-copy locations);
- confirm if any third parties are entrusted with the storage of your information; and
- understand where those third parties have your information.

Because this information is valuable to you, there is high risk that it will be attractive to others. Therefore, it is critically important to identify the potential threats to the security and integrity of the information and the locations in which it is stored.

Consider any internal threats. These could arise from an employee who inadvertently or innocently causes a situation. Employee error or well-intended but unsuccessful acts could be involved. Threats could also be due to inattentive or inadequately trained employees who cause an issue, or fail to identify, report, and escalate potential problems to the proper persons.

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

Internal threats could also be nefarious. For example, a rogue employee could steal or destroy data, or misuse and disrupt systems.

External threats must also be evaluated. Such actors could include a nation state, corporate spy, activist, ransom seeker, opportunist, or troublemaker.

In addition, third-party vendors engaged by you to hold data or perform services involving your data are an extension of your enterprise. The internal and external threats they may face could be threats to you.

It is therefore crucial to understand what and where your information assets are and to be mindful of the potential threat actors. You should concentrate on identifying the ways in which those actors might attack or affect your assets. Entry points could include the theft or other acquisition of credentials such as passwords or financial account information, the introduction of malware onto a system, deployment of ransomware, human error, failure to update system patches, failure of antivirus software or its implementation, the taking of paper or shredded paper records, the theft of computer hardware, and others.

These threats can create financial or other exposure, including costs to repair or replace information assets, costs to pay third parties for services, regulatory fines and penalties, business interruption or income loss, additional business expenses, reputational impact, litigation losses and costs, and others.

II. Risk Avoidance and Mitigation (*Preventive Care and Treatment Options*)

With the asset and threat landscape set out, preventive care can be gauged. Good privacy and cyber hygiene are sound business practices. They may, to some extent and for some companies, also be the law.

Entities should consider their document and information policies. These include both collection and retention policies. You should evaluate whether you have a valid business purpose to collect the information you do and the duration of that business purpose. If the information is useful for more than a very brief time, then you should evaluate storage options. Said differently, *do not collect what you do not need and do not retain what you no longer need*. Though there may be some exceptions for information that must legally be retained for a prescribed period of time or for which you have an ongoing business need, you will be in a better position if you appreciate the scope of the information you possess and have given or are giving thought to its disposition in the ordinary course of business.

For whatever information you have and for whatever period of time, there are a number of practices you should consider for the care of that information

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

or to address situations when your information assets may be vulnerable. Your consideration of your practices is not a one-time exercise. It is imperative that you revisit your information storage and retention practices regularly so that you can adjust them as needed to reflect your business and your risks at any given time.

You may also have legal, contractual, or other obligations that require certain practices or a certain level of preparedness. This chapter does not identify those obligations or identify specific steps for compliance. However, the issues in this chapter should be part of your compliance planning (for many of you, they already are).

We recognize that human and financial resources are not infinite. In assessing the practices for your purposes, we invite you to consider both technical and nontechnical measures and to be aware that some solutions have only modest costs.

We appreciate that you may have already discussed and undertaken a number of these measures. We also know that many of you will have done much more. The following is a starting point and we hope that for some of you the list provides food for thought, while it serves as a reminder for everyone. We encourage you to work with trusted advisors to develop or reassess the practices most appropriate for you. Regardless of where you are on the spectrum of readiness, you need to make sure that your practices reflect your own business, your own risk assessment, and your own compliance activities.

A. Governance

Good privacy and cybersecurity practices must come from the top and be genuinely encouraged, supported, and enforced by the most senior personnel.

One such practice is to have an incident preparedness and response plan[2] in place that has been endorsed internally and was developed with appropriate input, possibly including external professional service providers. The plan should be located in a place and format in which it can be accessed as needed. It should be reviewed regularly and updated as needed.

B. Information Management

In addition to the already discussed importance of procedures for the collection and retention of information, you should discuss, memorialize, and

2. For a more detailed discussion about the development of an incident response plan, see Chapter 3 ("How to Prepare for and Respond to Cybersecurity Attacks").

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

enforce procedures governing access to and use of various categories of information.

You should conduct due diligence in hiring and supervising the vendors you engage and to which you entrust information. To the extent you are able to negotiate the terms of your contracts with such vendors, the contracts should make clear what protection information will be given, the parties' respective obligations for security, the parties' respective rights and obligations in the event of any privacy or cybersecurity incident, and so on.

C. Technology and Related Practices

Subject to your budget, you should have information technology and security staff (whether employees or outsourced) and hardware and software commensurate with the volume and sensitive nature of the information you possess.

Your system architecture is important and you should consider the cost-benefit analysis of connectivity among system components. Consider segregating data and systems where appropriate.

You will want to have established solid and consistent backup procedures.

You should also consider technological restrictions for incoming or outgoing data and website traffic in order to quantify and manage the risk of sending critical information. These technological restrictions can also reduce the risk of being hit with malware or other unwanted materials when receiving e-mails. Some steps, such as encryption, may also be required by law for certain information. Some restrictions may depend on the type, volume, source, and destination of data, or even on the e-mail domain (for example, be cautious about free e-mail account domains). You could choose to prohibit access to specified websites (including those free e-mail account domains) or to limit the ability to download certain programs or mobile applications (apps). You could also restrict the use of thumb drives or other external devices with a business desktop or laptop computer.

Other access considerations may include the extent to which system access is permitted and for whom. Such access might also be limited to particular segments for particular users. It could also be temporary. You may consider the use of multi-factor authentication to permit any access to your systems. You may also choose to deploy specific password protocols that would require passwords to be changed regularly, establish a minimum length, require use of certain characters, exclude use of certain common words and phrases (such as local sports team names, your city name, or the seasons of the year), and so on.

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

D. Checks and Audits

You may arrange for regular cybersecurity audits and testing. You can also consider the usage records and logs kept at your system level as information to evaluate your security and to have available in the event of an incident.

E. User Training and Restrictions

Employee training is essential. All users should receive education about the importance of strong privacy and cybersecurity practices. The consequences of failing to follow such practices should be made clear, both as to the organization and the user. Practices discussed in training could include password protection, recognizing phishing or other scam e-mails, confirming the e-mail addresses of senders, being cautious about clicking on attachments, and others. Training sessions should stress technology safeguards and precautions and help users to identify and, as appropriate, escalate incidents for further handling.

Despite preventive measures, circumstances may still arise that require attention from you and your information specialists. The treatments and responses should be tailored to the particular situation. For example, you may be obligated or elect to take technical remedial steps. You should also be aware that your organization may become involved in legal or regulatory proceedings. You should consult with internal and external professionals to assist in your decision-making and in your implementation of measures.[3]

Depending on the type of insurance you have, your insurers may be able to connect you to skilled external professionals having expertise applicable to a specific scenario you are experiencing. This chapter now turns to insurance, a key component of any risk management strategy.

III. Risk Transfer (*Insurance*)

Insurance is a familiar tool. People insure their homes, their vehicles, their health, their lives, and more. Pursuant to the terms and conditions of an insurance policy, the policyholder, for the price of the premium, transfers the risk described by the policy to the insurer. For example, privacy and cybersecurity

3. Various specific steps concerning incident response, breach notification obligations, and cyber extortion (ransomware) are discussed in Chapter 3 ("How to Prepare for and Respond to Cybersecurity Attacks").

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

risks and their resulting losses can be the subject of insurance. This discussion focuses on insurance policies provided by commercial insurers.[4]

You should consult with your risk management professionals, including your in-house colleagues who work with insurance, an insurance agent, an insurance broker, outside counsel, a consultant, or others. They should identify your existing lines of insurance coverage and those lines' terms, conditions, and limits. You and they should consider whether the kinds of potential risks discussed in this chapter could potentially be covered under your existing coverage or whether additional coverage should be considered. Taking into account your privacy and cybersecurity risks, a related question is whether your existing coverage provides adequate limits with acceptable retention or deductible obligations. Based on that evaluation, you can then consider whether to price or purchase additional kinds of insurance.

In recent years, more insurers have been offering more types of standalone insurance addressing privacy and cybersecurity risks. Although such policies are often referred to as "cyber insurance," that term suggests a uniformity that does not exist. The coverages available in the market vary markedly in wording and scope.

At the same time, insurers of other lines of insurance have been considering, sometimes at the direction of regulators, the language of their noncyber policies to assess whether there may be some coverage for some types of cybersecurity situations or losses.[5]

This portion of the chapter broadly describes the different kinds of insurance. It also notes the important steps to consider about your insurance in the event of a potential privacy or cybersecurity loss.

---

4. It should be noted that risk transfer can also take the form of indemnification provisions between two or more parties. For example, a contract between a business and a vendor that holds the business's electronic data may contain language indicating which party does what if there is a disclosure or theft of that data. It is also possible that a contract could require one or more of the parties to the contract to purchase specified insurance. Although these types of risk transfer are not discussed here, you should evaluate all existing and new contracts to determine if such provisions should exist (if they do not) or if existing provisions are sufficient and acceptable to you (to the extent you have any ability to negotiate the terms).

5. This chapter's discussion of insurance is only general in nature. No specific insurer's policies are discussed. No specific policy language is evaluated. The authors do not endorse any particular insurer or insurance product. The terms, conditions, exclusions, and limits of liability of any policy can vary considerably. The enforceability of any policy's language by a court will depend on a number of factors, including the language itself, the facts surrounding the claim and the dispute, and the jurisdiction's law that does or may apply.

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

A. Cyber Policies

As noted, there is a variety of types of cyber insurance coverages. You can work with your risk management professionals to consider the particular ones most important to your enterprise. Some of the kinds of insuring agreements you may encounter are discussed later in this section.

You will want to be familiar with the terms and conditions of your policy. Definitions of key terms may be different under different insurers' wordings. For example, some coverages are for incidents affecting computer systems you own or lease, whereas others may extend coverage to incidents affecting the computer systems of third parties you contract with to store your data. You and your risk management professionals should focus on these kinds of distinctions before you choose a policy. One policy is not inherently better than any other, particularly when taking the amount of the premium and limits into account, but you should be aware of the language of the options as you decide what policy to buy or whether to purchase any such policy.

Importantly, regardless of the cyber policy you purchase, you should understand your rights and obligations under that policy.

You should know how and when notice is to be made—and you should know this before there is any incident requiring notice. Have that contact information readily available in the event of a situation for which you may want to seek coverage; consider including it in the text of your incident response plan.

You should also pay attention to the retention or deductible for which you are responsible under your policy. This may be a monetary amount for some insuring agreements and may vary notably among insurers' insuring agreements. It is also possible that the retention, depending on the insuring agreement involved, may be in terms of a number of people or a number of hours.

You should note which of the insuring agreements require you to first pay for a particular type of loss with the policy then reimbursing you. In addition, for some coverages to apply, policy language may require that you obtain the insurer's prior consent (and sometimes written consent) before incurring covered costs.

You will also want to be aware of the limits of your policy. There may be per-incident or per-claim limits on liability as well as an aggregate limit that caps the covered amounts the insurer will pay for all claims. Some coverages may be subject to sublimits that cap the coverage amounts for those particular insuring agreements. These caps can be monetary amounts, but they may also be keyed to a number of individuals, depending on the insuring agreement.

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

A potentially valuable aspect of some policies is that they provide you with access to services when there has been a suspected or known cyber attack or other incident that resulted or may result in a suspected or known disclosure of protected information. These services could include forensics firms to assess the technical details of whether and how your computer systems were infiltrated and whether protected information was accessed or copied. The policies may also offer you options for privacy counsel you can engage to help determine whether you have any notification obligations under federal, state, or other law. Public relations and crisis management services may also be available. There may also be coverage for notification costs, call centers, and credit monitoring. In most instances, insurers offering these services will require you to choose from among service providers on a list they provide. The insurers will have vetted these firms and negotiated rates for the benefit of their insureds.

Policies may include third-party insuring agreements for claims made against you by third parties who allege they have been injured as a result of privacy or cybersecurity situations caused by you. Subject to the terms of a policy, these may include, for example, claims or lawsuits brought by individuals who contend they are entitled to damages as a result of loss of their data, a violation of a privacy practice, or some other circumstance. It could also encompass media-related exposures such as postings on your social media that someone asserts violates their right to privacy.

Data or privacy incidents could also be the subject of proceedings initiated by a regulator who alleges violations of federal, state, or other legal authority. The definition of "proceedings" in a policy could include requests or demands for information from a regulator in addition to a formal inquiry or administrative hearing. Depending on the particular policy language, the legal authority at issue could include that in the U.S., the United Kingdom, the European Union, and perhaps elsewhere. There may also be coverage for certain losses from industry standards, such as Payment Card Industry (PCI) contractual assessments, that are often associated with incidents concerning personal information involving credit card numbers.

In addition, a number of cyber insurance policies include cyber extortion coverage, although it may apply only to certain types of attacks and may be affected by various exclusions (for example, for bodily injury or property damage). With such coverage, a policyholder usually must timely notify the insured of a demand or possible demand and the insurer typically must provide consent before any ransom offer or payment is made.

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

First-party coverages may include payment of amounts to restore or rebuild a system or a data population. Depending on the terms of your policy, there may be coverage for the restoration of the data and also for certain hardware and software replacements. A number of policies may provide coverage to restore you to the position you were in before an incident, but not for upgrades or betterment. Policies may not provide coverage for the value of the time you or your personnel devote to addressing an incident or re-entering data, but there may be coverage under some policies for the reasonable and necessary costs for third-party vendors to do so.

Some policies may afford coverage for business interruption or business income loss. As with all coverages, the particular language of the policy must be examined. You may need to identify your usual operating expenses, additional expenses you incurred as a result of an incident, patients you were not able to see due to the situation, patients you were not able to ever reschedule, prospective patients you could not take on while your systems were down, and more. You may wish to consider in advance whether your accounting or scheduling tools can produce the kind of reports you may want to have to support any future business interruption loss claim.

As discussed earlier, in addition to cyber insurance policies, other lines of coverage may be implicated for particular types of losses, although the extent to which these other lines may respond usually depends on the specific policy language, the facts of the situation, and the jurisdictions' law that may apply. These are described generally in the next section. In the event of any privacy or cybersecurity incident, you should discuss with your risk management professionals which of your policies should be put on notice.

B. Property Policies

First-party property policies, which usually cover physical damage to real and personal property and may (depending on their terms) also provide coverage for resulting business interruption, may offer potential insurance coverage for those who sustain business interruption losses, or costs for replacement of a computer system or data storage unit as a result of an incident. However, such claims may require some indication of physical damage to the computer system involved, or an express provision for coverage of replacement costs for loss of electronic data. Such policies typically cover "direct physical loss or damage to" or "loss of use of" insured property caused by a covered cause of loss. "Physical" is generally construed to mean "tangible," and there have been some court disputes over whether data is "tangible" property or over "loss of use" following a system attack.

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

Furthermore, policy exclusions could specifically exclude or limit coverage of electronic data and other "valuable papers and records." Exclusions could also prohibit alleged property damage resulting from malware, ransomware, or other system attacks. Business interruption coverage is generally required to result from damage to or destruction of property caused by a loss otherwise covered under the policy.

C. Fidelity and Crime Policies

Fidelity and crime insurance policies generally protect organizations from the loss of money, securities, or inventory resulting from employee crime. Common fidelity/crime insurance claims allege employee dishonesty, embezzlement, forgery, robbery, safe burglary, computer fraud, wire transfer fraud, counterfeiting, and other criminal acts.

Data incidents may involve theft and other criminal conduct by employees, such as theft of laptops or other computer equipment containing personal information or other confidential data. Thus, depending on its terms and exclusions, fidelity insurance may be triggered. Moreover, some fidelity or crime insurance policies may expressly provide for computer crime coverage in the form of a computer fraud endorsement, whereas others may contain exclusions that limit or preclude such coverage. Whether such an endorsement would provide coverage to the insured company for its losses and claim expenses arising from a data incident will depend on the policy terms, including if there is an exclusion for loss of electronic data, and the jurisdiction considering the issue of coverage.

Crime policies may be implicated in one of the hottest areas of cybercrime: socially engineered access to e-mail accounts or systems or even just information sufficient to have an e-mail from an external source appear genuine. An example is spoofed e-mails—ostensibly from an authorized corporate official—instructing an employee to transfer funds out of the company. Entities and a number of court decisions have wrestled with the legal question of whether the fact that the scam occurs by means of e-mail and thus a computer turns the scam into a covered loss.

D. Commercial General Liability Policies

An insured entity subjected to a lawsuit in connection with a data incident it suffers may tender the defense of that suit under its commercial general liability (CGL) policy.

Coverage A of a CGL policy typically provides that "we will pay those sums that the insured becomes legally obligated to pay as damages because of 'bodily injury' or 'property damage' to which this insurance applies."

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

"Property damage" is typically defined as "physical injury to tangible property, including all resulting loss of use of that property," and "loss of use of tangible property that is not physically injured."

In data incident cases, the focus of analysis as to whether there is coverage, or at least sufficient allegations to trigger a duty to defend, under Coverage A is generally on its "property damage" prong. Because of the required component of "tangible property," it is usually considered unlikely that lawsuits related to a typical alleged failure of electronic data security would be covered under Coverage A, on the basis that electronic data is not tangible property.

Furthermore, Coverage A also applies to "bodily injury." Third-party claims often include an emotional distress component. Thus, if a policy or governing law defines "bodily injury" as including emotional distress, there potentially could be a claim for coverage for that aspect of the alleged damages. However, although the "tangible property" barrier would not apply to such a claim, the insured would still have to demonstrate that the "bodily injury" was caused by an "occurrence" and that exclusions in the policy, such as data-related exclusions, do not apply. The potential for coverage may be more likely for data breaches and other cyber incidents directly causing demonstrable bodily injury, such as those involving computer-controlled medical equipment that affects medical care of individuals, rather than for the typical electronic data incident involving personal information.

One can also consider Coverage B, Personal and Advertising Injury coverage, which is limited to injuries arising out of certain enumerated offenses. In some policies, among these is typically "injury … arising out of … oral or written publication, in any manner, of material that violates a person's right of privacy." One would need to demonstrate, among other things, at least a potential that the data incident in issue constituted a "publication" and, separately, that such publication violated the data owner's "right of privacy." Courts have come to different conclusions about whether there is a "publication" in the context of a third party accessing or taking information, as opposed to any affirmative dissemination by the insured. Even if there were a "publication," however, there may be exclusions, such as an exclusion for alleged losses arising out of violations of particular statutes, which would otherwise serve to preclude coverage. In addition, there could be consideration of whether statutory fines or penalties are "damages" under the policy and other potential issues.

E. Professional Liability/E&O

Most professionals and entities engaged in providing services to others have errors and omissions (E&O) liability policies in place that they look to for a

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

defense and indemnity when a claim is asserted against them by their clients. When a data incident arguably occurs within the scope of covered services, such an insured may look to its professional liability/E&O insurer to at least provide a defense to any third-party claims arising from the incident. Thus, for example, a healthcare organization or professional that improperly discloses patient information, disposes of or loses patient files, or is otherwise subject to a data incident may try to seek coverage under its professional liability/E&O policies.

Often the coverage issues include, among others, whether the claim is within the scope of covered services, whether the insured's error that caused the alleged damage falls under the policy's definition of "wrongful act," whether there are alleged to be "damages" covered by the policy, whether contractual liability exclusions apply to indemnity claims, and whether there is an exclusion directed at data breach or other security or information claims.

F. Directors and Officers (D&O)

Large publicized data breaches and other privacy or cyber incidents that involve publicly traded companies may result in alleged drops in companies' stock prices or other large financial losses. Companies and their directors and officers faced with such a data breach or other type of cyber attack or incident may also encounter the type of securities/D&O claims that frequently accompany a significant and unexpected fall in stock prices and allegations of failure to disclose a material risk.

Furthermore, with the increasing issuance by state and federal agencies of data security regulations requiring the institution of data security protocols by companies, some of which expressly require board review of data protection plans and procedures, there may be an increase in D&O claims for all types of companies within their purview.

If a data breach, for example, leads to a suit against the allegedly responsible directors or officers by the owners of the compromised data—or by shareholders if the breach leads to a large loss to the insured company—, those directors and officers may look to their D&O policies to see if there is coverage. Similarly, in the event of a securities action, the targeted company may look to any entity coverage provided by such policies.

As to exclusions, it is possible, for instance, that the D&O policy at issue may exclude claims arising from violations of privacy rights or cyber events.

G. Kidnap and Ransom/Cyber Extortion

Corporations and individuals operating in high-risk areas around the world often carry kidnap and ransom coverage. Such policies typically provide

©2021 by the American Bar Association. Reprinted with permission. All rights reserved. This information any or portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

indemnity in connection with ransom payments and personal accident losses caused by kidnapping incidents. Such policies may also cover extortion, including extortion related to a threatened introduction to or activation of a computer virus in the insured's computer system unless a ransom is paid. Depending on the policy's scope of coverage, including how the policy defines "virus," such "ransomware" coverage may extend to a hacker's threatened or actual use of software to capture or compromise private data.

IV. Conclusion (*The Prescription*)

Risk management is vital to the well-being of any organization. Be aware of your current conditions. Be mindful of what you would like to improve. Be conscious of the resources and practices that can improve your health. Be alert to risks. Be ready to respond when necessary. Be prepared to engage your insurers as appropriate. Be well.