# Cyber Liability

## 4 Components of Cyber Risk Management

If your company stores information digitally, it's important to develop a cyber risk management program that will help minimize the likelihood of a data breach and reduce potential losses if a breach does occur. Effective cyber risk management requires the planning and execution of four key components: prevention, disclosure, crisis management and insurance coverage.

### 1. Prevention

Your data breach prevention strategies may include encrypting all devices used by your employees, such as laptops, tablets and smartphones. Encrypting these devices will prevent unauthorized access if such technology is lost or stolen. Unencrypted devices are often excluded from coverage under cyber insurance, so make sure you know whether you need to encrypt all workplace technology. Your prevention strategies may also include educating employees about phishing and other social engineering scams. Remind them not to click on, respond to or download anything that looks suspicious or seems too good to be true. It's best to analyze your cyber risks from three different perspectives: technology, people and processes. This risk assessment will give you a clear picture of potential holes in the overall security of your IT infrastructure. Revisit this assessment regularly, as risks can evolve and emerge over time.

### 2. Disclosure

If you experience a data breach, you may be legally required to notify certain parties. In particular, certain state laws and international legislation require companies to inform anyone whose personal data was exposed by a breach. If your company is publicly traded, guidelines issued by the U.S. Securities and Exchange Commission (SEC) make it clear that you must report cybersecurity incidents to stockholders—even when your company is only at risk of an incident. The SEC advises timely, comprehensive and accurate disclosure about risks and events that would be important for an investor or client to know. It's essential to evaluate what information and how much detail should be released. Notifying a broad base about a breach when it's not required could cause unnecessary concern for those who have not been affected by the incident. However, a large-scale breach may require more than just assessing and disclosing the information. Depending on its sensitivity, you may have to destroy or alter data.

### 3. Crisis Management

Preparedness is key when developing your cyber risk management program. When you experience a data breach, you need to be ready to respond quickly and appropriately. This is where your crisis management and response plan comes into play.

This plan involves having procedures in place to determine when and how the breach occurred, what information was obtained and which parties were affected. From there, it's critical to assess the risks you face because of the data breach and how you will mitigate those risks. While managing a crisis, let your stakeholders know what actions you are taking, but also be sure you're not disclosing too much information; it's a delicate balance. Focus on improving future actions to restore trust and avoid lasting reputational damage. Be sure to work with lawyers, risk managers and IT experts—whether these professionals are in-house or external—to create and refine your plan. Everyone should be on board and know their responsibilities when a data breach happens.

### 4. Insurance Coverage

Your cyber risk management program should include cyber insurance coverage that fits your company's needs. This coverage is specifically designed to address the risks associated with using modern technology in the workplace—risks that other types of commercial insurance policies simply won't cover. The level of coverage your company needs is based on your specific operations and can vary depending on your exposure.

In any case, your cyber insurance policy can be tailored to fit your unique situation and can be written to include protection for certain data breach-related losses. Contact us today for additional risk management guidance and insurance solutions.

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.