Both experience and research confirm that the greatest risk to a company comes from basic cybersecurity’s failure to block and tackle. A data breach is much more likely to happen due to something simple—such as employee negligence, a lost or stolen device, or falling for a social engineering scheme—than it is because of a sophisticated cyberattack.

Potential risks vary across sectors; however, the Ponemon Institute’s Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data shows the magnitude of the evolving cyberrisk in this industry alone: “Over the past two years, 91 percent of healthcare organizations reported at least one breach, 39 percent reported two to five data breaches, and 40 percent had more than five data breaches.” The severe impact and the notoriety of these breaches are compelling examples of why lawyers must understand the risks so we can advise clients on how to protect their businesses.

What is cyber insurance? Cyber liability insurance has been around for more than 35 years, having been first introduced in the 1980s. In those days, it was referred to as errors and omissions insurance, which included issues such as virus attacks or illegal access to a system. Today, cyber coverage can mean different things to different people. The term “cyber liability” encompasses the components of this risk. This is to say that all companies that use a computer, receive, store, or transmit electronic data, or connect to the Internet are exposed to it. Cyber insurance is designed to cover cyber liability, among other things.

How will experienced insurance professionals help? Experienced professionals offer advice on solutions that can help protect your client from potentially suffering a large financial or reputational loss due to cyberrisk. They will do this by first helping clients identify the risks associated with their business operations. This requires taking a step back from the hazard risk, or the risks generally covered via insurance, and looking at risk as a whole. They will look at it from business, strategic, and hazard perspectives. From there, they will help educate your clients on how to manage each of their risks through prevention, mitigation, transfer, financing, and assumption of risk. For cyber liability, they will focus on risk mitigation and risk financing techniques.

To assist in this process, there are some key questions that clients should consider:

- How would a cyberattack, data breach, or data hijack impact their ongoing operations?
- How much would their reputation suffer?
- Do they have a plan in place to respond to a breach and help mitigate loss in the event of a breach?

What kinds of policies cover cyber liability? Usually there is limited coverage for cyber liability under general commercial policies. Notable cases have driven the need to standardize cyber liability insurance products as well as revamp current general liability policy language.

However, the legal wrangling over these issues is still unresolved, and the insurance industry has responded by taking steps to carve out “data-related liability” from the commercial general liability insurance policies via a new exclusion. This has helped to eliminate vague policy language but has also created a need for some companies to purchase additional policies to prevent gaps in coverage.

Every business has its own vulnerabilities, and there is no one-size-fits-all approach. There are, however, several core elements for which a quality cyber insurance policy should provide coverage, including the following first-party costs:

- legal and forensic services to determine whether a breach occurred and to assist with regulatory compliance if a breach is verified;
- notification of affected customers and employees;
- customer credit monitoring and identity protection services;
- crisis management and public relations to educate the company’s customers about the breach;
- business interruption expenses, such as additional staff, rented or leased equipment, third-party services, and additional labor arising from a covered claim; and
- cyber extortion reimbursement for perils, including credible threats to introduce malicious code; pharm and phish customer systems; or corrupt, damage, or destroy their computer system.

Such a policy should also provide coverage for the following third-party defense and liability costs:

- judgments, civil awards, or settlements following a data breach;
- electronic media liability, including infringement of copyright, domain name, trade name, service mark, or slogan on an intranet or Internet site; and
- potential employee privacy liability as well as network security and privacy liability.

It is important to review the policy lan-
guage for basic insurance coverage issues, such as deductibles, sub-limits, and total limits, as well as specific exclusions.

There are a few key items that may not be covered, including:
- reputational harm;
- loss of future revenue (such as decreased sales due to customers staying away after a data breach);
- costs to improve internal technology systems; and
- lost value of the company’s own intellectual property.

Not every attorney needs to be an expert on cyber law; however, a basic familiarity with the issues is helpful. As your clients’ trusted adviser, it is important for you to have enough understanding of cyber risk to be able to consider raising these issues with clients and advising them on how they can seek additional protection. This is just a cornerstone of practical lawyer-ing in the 21st century. TBJ

Notes
5. Id.

This article has been edited and reprinted with permission of Circuits and the authors.

SHAWN TUMA is a business lawyer in cybersecurity, computer fraud, and data privacy law. He is a partner in the Cybersecurity and Data Privacy Law Group at Scheef & Stone.

KATTI SMITH is an insurance professional working as a senior business development manager with AIG Property Casualty. During her nearly 15-year career, she has obtained several industry specific designations, including her Chartered Property Casualty Underwriter, Registered Professional Liability Underwriter, and Associate in Risk Management. Her focus is on sales and marketing for commercial and professional lines of business.