This Practice Note examines issues related to obtaining insurance coverage specific to data breach risks, including the need for coverage, whether coverage may be available under other types of policies, the scope of cyber coverage and key considerations when applying for and selecting coverage.

Coverage for data breach-related expenses under traditional commercial insurance policies has become increasingly uncertain. Cyber insurance addresses gaps in coverage that may arise under traditional commercial policies. Their primary purpose is to protect against data loss and exposure of personally identifiable information (PII).

In the early 2000s, insurers began to offer insurance policies specifically geared towards protecting against financial losses from data breaches. These early policies covered:

- Business interruption.
- Data asset loss, extortion and crisis management costs.
- Liability arising out of a breach of computer systems.

After California passed the first state data breach notification law in 2003 and nearly every state followed suit, the need for insurance coverage specifically designed to address breach-related costs and liabilities increased.

Comparing and selecting cyber coverage is rarely straightforward given the lack of policy standardization and the complex nature of data risks. However, cyber risk is increasing and securing an appropriate policy that provides coverage for a data breach is an important part of a business's risk management program. This Note discusses:

- An overview of cyber insurance and data breach risks.
- Coverage under traditional insurance policies.
- Typical cyber insurance coverage for data breaches.
- Assessing risk and coverage needs.
- Applying for and selecting cyber insurance coverage for data breaches.

**BENEFITS OF CYBER INSURANCE**

Cyber insurance provides coverage for many of the expenses that may arise from a data breach involving PII, including:

- Computer forensics.
- Privacy or security breach notification and response.
- Crisis management.
- Data loss or destruction.

A typical cyber policy includes insuring agreements relating to more than one of these coverages and may include other insuring agreements not principally directed at risks to PII (see Box, Other Cyber Coverages). While many of the considerations regarding assessing the need for and selecting coverage overlap, this Note focuses on issues related to insurance coverage in the context of a data breach that involves PII.

**DATA BREACH RISKS**

Data breach incidents have become more common and more costly in recent years and have affected almost every industry, including not only technology and communications, but also retail, healthcare, energy, finance and hospitality, among others.

Data breaches affecting PII come in many forms and may be the result of:

- External threats, including:
  - hacking incidents directed at stealing PII for economic gain; or
  - theft of hardware or other media containing PII, whether or not it can be established that the media was stolen for the PII.

- Internal threats, including:
  - employee negligence, such as the loss of a laptop or other media containing PII;
  - system glitches that improperly expose PII, such as through postings on an external-facing website; or
  - improper disposal of hardware containing PII.
THE INSURABLE COSTS OF A DATA BREACH

Regardless of the source of the breach, the costs associated with a data breach incident that compromises PII can be astronomical (see Box, The High Price of a Data Breach).

There are typically three types of insurable expenses associated with data breach incidents:
- Response and investigation costs, including data restoration.
- Litigation defense and damages.
- Regulatory defense and penalties.

RESPONSE COSTS

A variety of federal and state laws may require businesses to promptly notify customers if their information has been compromised. Companies need to respond quickly and forcefully to minimize disruption to and loss of business and to avoid or mitigate legal liability.

Response costs may include:
- Hiring counsel to analyze legal requirements.
- Hiring a forensics firm to investigate the incident or recreate the data.
- Mailing and printing notice letters to those affected by the breach.
- Setting up a call center to respond to customer inquiries.
- Providing credit monitoring or other mitigation services.
- Retaining public relations professionals or crisis managers.

For more on data breach notification, see Practice Note, Privacy & Data Security: Breach Notification (www.practicallaw.com/3-501-1474).

LITIGATION DEFENSE AND DAMAGES

When a business suffers a data breach, class action litigation often follows. Law suits may assert claims for:
- Federal or state statutory violations, including consumer protection, privacy and breach notification statutes.
- Common law negligence, fraud or breach of contract.

These suits may seek statutory or other damages and an order that the defendant pay for mitigation products, such as credit monitoring. Because of the large size of the putative classes in these cases, the claimed damages can be large.

In addition, data breaches may spawn derivative suits or other litigation, such as contractual disputes with vendors or, in breaches of payment card information, disputes with other members of the card system or the card brands.

Even though most cases are resolved in the early stages, the costs of defense can easily reach hundreds of thousands of dollars or more. In addition, because of the cost to defend, defendants may settle these actions even if the plaintiffs' chance of success on the merits is small. For more information on data breach litigation, see Practice Note, Key Issues in Consumer Data Breach Litigation (www.practicallaw.com/5-582-9285).

REGULATORY AND OTHER COSTS AND PENALTIES

The exact nature of regulatory and other costs depend on:
- The breached entity's business or industry.
- The data affected.
- The jurisdictions in which the breached entity does business or in which it has customers.
- Any contractual obligations.

However, businesses that experience a breach may be subject to:
- Federal regulatory actions, including investigations, fines and penalties.
- State regulatory proceedings, often across multiple states, that may result in investigations, fines and penalties.
- Compliance costs, fines or penalties under rules that apply to the payment card industry (PCI) under various contracts.

COVERAGE UNDER TRADITIONAL POLICIES

While traditional commercial insurance coverage may provide some avenues to mitigate risk in a data breach, businesses may put themselves at risk if they rely on those policies for primary coverage for a data breach. Though some businesses have successfully made claims on traditional policies, relying on traditional policies for coverage for a data breach event has become increasingly uncertain.

SCOPE OF TRADITIONAL POLICIES

General commercial liability policies typically include three types of coverages:
- Coverage A, which covers bodily injury and property damage (for more information on Coverage A, see Practice Note, Commercial General Liability Insurance Policies: Property Damage and Bodily Injury Coverage (Coverage A) (www.practicallaw.com/9-507-2539)).
- Coverage B, which covers personal and advertising injury (for more information on Coverage B, see Practice Note, Commercial General Liability Insurance Policies: Personal and Advertising Injury Coverage (Coverage B) (www.practicallaw.com/0-507-2567)).
- Coverage C, which covers medical payments for bodily injury.

These policies typically define property damage as a physical injury to or the loss of use of tangible property, and many policies specify that electronic data is not tangible property. In addition, most policies also exclude damage to the insured's own property.

Accordingly, traditional commercial policies include definitions and other terms that could exclude losses associated with a data breach because the breach concerns either or both:
- Electronic data.
- Damage, such as through loss or hacking, to the insured's own property.

Nevertheless, some businesses have successfully made claims for data breach losses under their traditional policies, particularly under Coverage B. In addition, some insureds have successfully claimed for certain types of exposure under their employment practices liability
Further, the terms of cyber policies are often “manuscripted,” meaning that specific provisions tailored to the insured’s unique risks often result from negotiations between the insured and the insurer.

However, typical cyber policies on the market today include coverage for:

- The insured’s costs for responding to a data breach (see First-party Coverage).
- Damages and litigation expenses arising from actions against the insured following a data breach (see Third-party Coverage).

**NEW ISO ENDORSEMENTS**

The Insurance Services Office (ISO) periodically publishes standard insurance policy forms that insurers use widely. Where not used in their entirety, insurers adopt often the forms with substantial standardization.

As insurers started adding exclusions to their traditional commercial policies, ISO has approved new forms for optional endorsements that exclude coverage for personal and advertising injury claims arising from the access to or disclosure of confidential information. Specifically:

- **CG 21 08 05 14 (Exclusion: Access Or Disclosure Of Confidential Or Personal Information (Coverage B Only)).** This endorsement excludes coverage for personal and advertising injury arising out of any access to or disclosure of confidential or personal information even if the insured claims damages for:
  - notification costs;
  - credit monitoring expenses;
  - forensic investigation expenses;
  - public relations expenses; and
  - any other loss, cost or expense incurred due to the access to or disclosure of personal information.

- **CG 21 07 05 14 (Exclusion: Access Or Disclosure Of Confidential Or Personal Information And Data-related Liability: Limited Bodily Injury Exception Not Included).** This endorsement is similar to CG 21 08 05 14, but it also excludes coverage for bodily injury and property damage arising out of any access to or disclosure of confidential or personal information or the loss of or damage to electronic data.

- **CG 21 06 05 14 (Exclusion: Access Or Disclosure Of Confidential Or Personal Information And Data-related Liability: With Bodily Injury Exception).** This endorsement is similar to CG 21 07 05 14, except that bodily injury arising out of the loss of or damage to electronic data is not excluded.

ISO made these endorsements available in 2014, and they are expected to be widely adopted by insurers. (See ISO Comments on CGL Endorsements for Data Breach Liability Exclusions (July 18, 2014).)

**TYPICAL CYBER COVERAGE FOR DATA BREACHES**

Given the increased exposure and the uncertainty of coverage under traditional policies, demand for cyber insurance to mitigate data breach risk has increased dramatically over the last several years. However, cyber insurance is a developing product, and insurers have yet to adopt standard forms, which can make researching and comparing policies challenging.
undetected data breach when they are applying for coverage and attempt to secure coverage that might apply to any undetected events. In some cases, insurers may be willing to provide retroactive coverage for up to two years before writing the policy. However, whether or not an insurer will offer retroactive coverage is highly dependent on the insurer and the potential insured's unique risk profile.

**VARIATIONS ACROSS POLICIES**

The structure of cyber policies varies widely, which can make comparing policies extremely difficult for the prospective insured. Cyber policies often contain multiple insuring agreements, all with separate sub-limits and retentions. For example, a cyber policy may contain up to a dozen separate insuring agreements setting out coverage and the insured may have the option of selecting from the coverages.

Coverage differences across policies can be substantial and may include not only variations as to the standard items covered for notification and defense costs, but also variations in:

- The scope of territory covered.
- Aggregate policy limits and sub-limits.
- Self-insured retentions.
- Coverage periods.

In addition, although the scope of coverage may be similar across a variety of cyber policies, the actual insuring agreements that set out the scope of that coverage may be substantially different, and the same coverage that is included in one insuring agreement in one policy may be split across multiple insuring agreements in another, or the terms used across policies may be the same but have substantially different meanings.

Businesses must pay close attention to all policy terms to ensure they understand the scope of coverage and that it is adequate considering the business's needs and risk profile (see **Selecting Cyber Coverage**).

**EXCLUSIONARY PROVISIONS**

As with all insurance policies, insureds must carefully examine exclusions and other policy provisions that may limit coverage. Because of the lack of standardized forms, this is especially true when selecting cyber coverage.

**TYPICAL EXCLUSIONS**

Since the primary purpose of cyber insurance is to protect against the loss of intangible data and the exposure of personal information, cyber policies generally exclude damages arising out of:

- Bodily injury.
- Property damage.

Cyber policies also typically exclude coverage for claims arising out of various categories of violations, such as:

- Employment practices.
- Pollution.
- Antitrust violations.
- Employment Retirement Income Security Act (ERISA) violations.
- Telephone Consumer Protection Act violations.

In addition, policies may exclude coverage for:

- Intentional acts by directors and officers, regardless of whether they acted outside the scope of their employment and intended to harm the company.
- Unlawfully collecting personally identifiable non-public information.

Policies may also exclude coverage for incidents involving payment card data unless the business purchases an additional rider.

**DEFINITIONS AS EXCLUSIONS**

Exclusionary provisions may be contained within some definitions in cyber policies. The policy may define terms in a way to exclude coverage in potentially unexpected ways. Businesses must carefully review all defined terms to assess their effects on coverage to ensure they are not unintentionally selecting a policy that excludes desired coverage.

**SELECTING CYBER COVERAGE**

Entities considering cyber insurance should first fully assess their business operations (including contractual obligations) to determine their cyber risks and coverage needs.

**ASSESS CYBER RISK**

Selecting effective cyber coverage requires the business to consider the nature of cyber risks it faces. For instance, companies that collect and store PII may be concerned about notification and related expenses, while companies that store massive amounts of valuable data that is not PII might be concerned instead about the costs of restoring data destroyed during a data breach. Some businesses may have strong concerns about rogue employees and other insider threats, while others may primarily wish to insure against hackers and other outsider threats.

Assessing these risks requires amassing information from multiple stakeholders, including:

- Information technology (IT).
- The privacy or compliance office.
- Human resources (HR).
- Business operations.
- Legal and risk.

This cross-disciplinary approach is necessary to assess the following issues, which are critical in determining the business's cyber risk profile:

- **The nature of the data the business maintains.** Different risks are associated with different types of information. For instance, storing sensitive personal information of individuals, such as healthcare or financial information, presents a greater risk that the business will ultimately suffer a data breach that will require expensive individual notification of affected persons.

- **Legal obligations in the event of a data breach.** In addition to understanding the data it maintains, a business must understand what legal obligations it will have in the event of its breach. A myriad of legal and contractual obligations may apply. A business should consider, for example:

  - whether it owns the data or holds it as a vendor;
  - the jurisdictions in which it does business;
■ whether it operates in a highly regulated area; and
■ whether it has any indemnification obligations.

■ The cost to recreate data. In the event of a breach, data may need to be recreated either for operational or notification purposes or both.

■ The strength of the security program and control over data. While no security program can fully insulate against the risk of a data breach, the strength of the security program is relevant to assessing the level and nature of the risk. A business should consider, for example:
  ■ the nature and implementation of its information security program;
  ■ its physical security;
  ■ where it stores data, for instance in the cloud or on a third-party platform; and
  ■ whether it shares data with third parties.

■ Previous breaches or other security events. As part of any analysis of risk, businesses should consider those threats it has already faced, the costs incurred and the likelihood that the threat will arise again.

**ASSESS COVERAGE NEEDS**

Once the company understands its cyber risks, it should then review its existing insurance program to determine any gaps in coverage. Given the uncertainty of coverage for data breach incidents under legacy policies, companies should retain experienced coverage counsel to help with this assessment (see Coverage under Traditional Policies).

Selecting coverage entails comparing the business’s risk profile and gaps in coverage under its existing policies with the available coverage options, including manuscripted options. Developing hypothetical breach scenarios may be helpful in making this assessment.

In addition to the terms of coverage, businesses should consider:

■ Appropriate retroactive coverage for prior unknown breaches.
■ Appropriate retentions.
■ Appropriate limits and sub-limits (see Practice Note, Insurance Policies and Coverage: Overview: Deductibles or Self-Insured Retentions and Aggregate Policy Limits (www.practicallaw.com/9-505-0561)).
■ The cost of premiums.
■ The control the insurer retains over decision-making in responding to an incident.
■ Whether the insurer requires using panel counsel or vendors if an incident occurs, and if so, the strength and depth of the panels.

In selecting a policy, businesses should also be aware that in the event of a breach, some insurers assign a dedicated breach response manager to the claim who helps the insured navigate through a breach response. Businesses must assess whether this type of service is desirable when selecting coverage.

Some carriers offer risk management services as part of their coverage. These services may include, for example:

■ Security assessments or audits.
■ Incident response plan assessments.

■ Penetration testing.

While these services may be attractive, businesses should consider whether they actually add value or if others are already providing the services to the business. Excluding unneeded coverages may decrease premiums.

**APPLYING FOR CYBER COVERAGE**

Insurers typically require businesses applying for cyber insurance to complete a detailed underwriting application designed to convey the nature of the company’s risks to the prospective insurer. Because applications are comprehensive and seek information designed to identify multiple channels of cyber risk, the prospective insurer should include all relevant stakeholders in the process, including representatives from:

■ Legal and risk.
■ Privacy and compliance.
■ HR.
■ IT and information security.
■ Business operations.

**THE APPLICATION**

Cyber applications typically request detailed information regarding the nature of the business, its policies for holding and using data and its security program. Responding fully and accurately in completing the application may avoid coverage disputes.

In applying for coverage, businesses can expect to be required to provide information regarding prior data security incidents and specific information regarding its data security practices, for example:

■ The composition of the security team.
■ The percentage of total IT budget allocated to security.
■ Technical safeguards, including for example information regarding:
  ■ the use of encryption;
  ■ security assessments and audits;
  ■ relevant hardware and software the business uses, including firewalls; and
  ■ access control requirements.
■ Administrative and physical safeguards, including for example:
  ■ employee hiring and training practices; and
  ■ the applicant’s physical security controls (such as access cards, biometric access controls and data center access logs).
■ Issues related to third-party controls, such as:
  ■ audits of third-party service providers; and
  ■ vendor contracts.
■ The backup of data.

In addition, many insurers require applicants to attach relevant company policies, including:

■ Internal and external privacy and data use policies.
■ Network security and training policies.
■ Policies governing the appropriate use of network resources, the internet, e-mail and social media.
- Records and information management compliance policies.
- Data destruction policies.
- Incident response plans.

**RISK REVIEW**

Some insurers require applicants to undertake a security risk review before writing coverage. Businesses must consider not only whether they will pass the review, but also whether the review itself would compromise proprietary data or result in a privacy violation.

While both the risk review and the application process may take time, these processes provide the business with the opportunity to further examine its risk profile and to potentially identify weaknesses in its security programs.

**CONDITIONS OF COVERAGE**

Before writing coverage, insurers may expect applicants to reduce or limit their breach risk through a variety of means, including:
- Implementing encryption.
- Engaging in security audits.
- Deploying specific technical, administrative or other security enhancements.

Alternatively, some insurers may not require these measures as conditions of coverage, but they may offer reduced rates to applicants who choose to implement them.

While many of these security enhancements may be desirable in their own right, others may be costly and time-consuming to implement. Businesses should consider whether they can reasonably adhere to the insurer’s requirements and avoid purchasing a policy with conditions of coverage that are prohibitive based on the business’s nature and resources.

**POST-COVERAGE CONSIDERATIONS**

Once coverage is in place, businesses must:
- Understand any conditions of coverage and the claims process.
- Periodically monitor and evaluate the coverage in light of business needs and the changing cyber insurance market.

**NOTICE OF CLAIMS**

Virtually all insurance policies contain notification conditions. Regardless of whether the insured has secured cyber-specific coverage, it is sometimes unclear at the time of initial notice what coverages may potentially apply or whether the claims exceed primary policy limits.

An insured should consider all policies in effect when the claim is made and when conduct under the asserted claims for relief may have first occurred when providing notice. These may include:
- Primary policies, including any cyber-specific policy.
- Umbrella or excess policies.
- International commercial general liability (CGL) or umbrella policies.
- Cancelled policies.


**MONITORING COVERAGE AND AUDITING COMPLIANCE**

Businesses should review their cyber policies and needs frequently to ensure they maintain appropriate coverage and minimize costs as more insurers enter the market and new policy options become available.

In addition, if the business selected a policy that includes conditions of coverage, it should implement a program to periodically audit and document its compliance with those conditions.

**MERGER AND ACQUISITION CONSIDERATIONS**

Businesses contemplating a merger or other similar transaction should carefully review their cyber coverage to ascertain how the deal would affect coverage. For example, depending on the policy and circumstances of the transaction, a cyber policy may require insureds to:
- Provide notice before the acquisition.
- Obtain the insurer’s written consent.
- Agree to pay any additional premium.

Additionally, divesting interest in a subsidiary may also divest the subsidiary of cyber coverage. Cyber policies may also contain provisions that trigger upon a takeover of the named insured. Considering these provisions early in the transaction helps facilitate compliance with any requirements.

**OTHER CYBER COVERAGES**

Cyber insurance can cover more than data breach response costs, and businesses should carefully consider the need for additional coverages based on their risk profiles. Cyber policies often include or provide the option to add coverage for a range of information security and online risks, including:
- Network security.
- Media liability, which covers claims related to slander, libel and defamation.
- Extortion liability.
- Business interruption costs.

In addition, new cyber threats continue to emerge, some of which go beyond the risks that most cyber policies traditionally cover. For instance, state-sponsored or terrorist hackers that target critical infrastructure and aim to disrupt or destroy power plants, water-treatment facilities, telecommunications systems and other infrastructure present a growing threat. The Department of Homeland Security recently acknowledged a specific threat to critical infrastructure and alerted operators to a Russian hacking group that was trying to sabotage the energy sector in the US and Europe.

Most cyber policies exclude coverage for property damage and therefore would not cover these critical infrastructure threats. Some insurers have responded by offering additional coverage specifically geared toward the critical infrastructure market that cover property damage and bodily injury liability arising from cyber attacks. Potential insureds that may be prone to these risks should consider whether these new policies would be beneficial.
**THE HIGH PRICE OF A DATA BREACH**

While the $148 million Target has already spent on data breach costs has made headlines, even an ordinary data breach can cost millions. According to the Ponemon Institute, the average US organizational cost for a single data breach of fewer than 100,000 records in 2013 was $5.85 million, with 33% of the costs being direct costs, which are typically the insurable costs, and over $500,000 spent on post-breach notification alone.

The Ponemon Institute estimates that the costs of business disruption, which includes reputational damages and customer churn (the proportion of customers who abandon the business) at $238,717. Costs associated with DDoS attacks, in which hackers render their target’s website, network, server or application resources unusable, can also be devastating, at an estimated average cost of $22,000 per minute of downtime.

**SONY CORPORATION**

In March 2014, a New York trial court issued a bench ruling that hacking was "publication" under a commercial general policy. Sony made a claim under its general commercial policy for litigation that arose from a well publicized 2011 hacking event under a provision that covered liability for "oral or written publication in any manner of [the] material that violates a person’s right of privacy." Though the trial court found that the hacking was publication, it also found that for any publication to be covered by the policy, it had to be publication by the insured itself. The case is currently on appeal. ([Zurich Am. Ins. Co. v. Sony Corp., 651982/2011 (Sup. Ct. N.Y. Co. 2014).](#)

**CORCINO & ASSOCIATES**

By contrast, in November 2013, the US District Court for the Central District of California found that a general commercial liability policy provided coverage for a privacy breach.

Corcino & Associates provided medical information to a job applicant who posted the data on the internet and an affected person sued. Corcino made a claim on its comprehensive general liability policy issued by Hartford. Hartford denied Corcino’s damages claim under a policy exclusion that barred recovery for violations of statutorily created rights and brought a declaratory judgment action seeking a declaration about the exclusion.

The court held that even though the plaintiffs in the underlying litigation were suing under various statutes, the confidentiality of medical information was well-established and not created by statute. ([Hartford Cas. Ins. Co. v. Corcino & Assocs., No. CV 13-3728 GAF (JCX), 2013 WL 5687527 (C.D. Cal. Oct. 7, 2013).](#)

**RECENT COVERAGE DISPUTES**

Over the past several years, courts have issued conflicting decisions when asked to determine whether traditional policies cover data breach losses. These cases often turn on subtle variations or interpretations of policy language or state law.

**RECALL TOTAL INFORMATION MANAGEMENT**

In February 2014, a Connecticut appeals court found that a general commercial liability policy did not provide coverage when tapes storing personal information were stolen. The insurer denied coverage when the insured made a claim under a provision that defined personal injury as "injury, other than bodily injury, property damage or advertising injury, caused by an offense of . . . electronic, oral, written or other publication of material that . . . violates a person's right to privacy."

The court found that the policy did not cover the incident because, despite the theft of the information, there was no evidence that any of the information on the tapes was "published." ([Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 83 A.3d 664 (Conn. App. Ct. 2014).](#)

**ABOUT PRACTICAL LAW**

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at practicallaw.com. For more information or to schedule training, call 888.529.6397 or e-mail training.practicallaw@thomsonreuters.com.