A Brief Guide to Mitigating Cyber-Risk:

Proactive Steps that Every Business Should Consider

By Tucker Bohren and William Africk

This article will focus on the privacy obligations of financial institutions in light of the five state consumer privacy laws that are scheduled to take effect in 2023.

The benefits that the internet provides to people and businesses come with a growing risk of and exposure to cyber incidents such as security breaches and privacy breaches. The news consistently reports on a host of incidents involving phishing, malware, social engineering attacks, data breaches, ransomware, and encryption. Security and privacy breaches have become more common and more costly in recent years and have affected nearly every industry, including healthcare, business and professional services, finance, insurance, education, manufacturing, retail, and energy, among others. (See Ted Kobus, BakerHostetler 2022 Data Security Incident Response Report, p.3.) A cyber incident can sink a company or its reputation, and the threat actors perpetrating these crimes know it.

In 2021, the number of security breaches, privacy breaches, and ransom demands increased while the average size of targeted companies decreased. (In the first half of 2021, a larger number of claims targeting small- and mid-size businesses resulted in the frequency of cyber-insurance claims increasing by 57% for organizations with 250 employees or less. See Coalition H1 2021 Cyber-Insurance Claims Report, p 3-4.) Considering these trends, cybersecurity and risk management is as important as ever for all modern businesses, regardless of the goods or services sold, their size and pedigree, or their actual or aspirational customer base. All prudent businesses should treat cyber risk management like any other risk: evaluate and accept the risk and implement a multi-pronged system to plan for the worst while minimizing exposure and liability.

What Does a Security Breach Look Like?

Consider Jane, a solo practitioner attorney from a prominent local family. She worked hard to build a small practice. Barring any major setbacks, Jane's business is growing into what she has envisioned—a thriving practice. She has a staff of four including two paralegals, an accountant and social media coordinator.

One Saturday morning, Jane finds that her business' website now features graphic, offensive, and, maybe even, illegal pictures. She immediately calls her social media coordinator who does not answer. Even though Jane does not know how to change her webpage, she tries to log-in. Predictably, the password and username have been changed. Jane's website is compromised; but she has not received a ransom demand—yet—and her e-mail account and e-files appear to be in order.

Although not exactly tech savvy, Jane understands the potential risks of a cyber breach but not necessarily the reality of what a "breach" involves. As a lawyer, she regularly handles personal identifying information ("PII") and Protected Health Information ("PHI") of her clients; witnesses in their cases; adverse parties, and vendors. Some examples of PII include social security numbers, addresses, and account numbers. To the extent a threat actor has gained access to the PII or PHI within Jane's records, she and her firm may face exposure from regulatory agencies, cli-

Tucker Bohren is an attorney with Phelps Dunbar. He prevents, solves, and litigates insurance coverage disputes for domestic and international carriers. Tucker handles first-party and third-party claims and lawsuits involving cyber, commercial general liability, property, employer liability, and errors & omissions insurance policies. Tucker lives in New Orleans, Louisiana with his wife and two children. **William Africk** is an attorney at O'Bryon & Schnabel, PLC, a boutique litigation firm in New Orleans. As a former public defender, Will is naturally protective of individuals' privacy rights. This background led to Will's appreciation of being able to explain complicated concepts simply, whether it be to clients, courts or on cross-examination. Will advises his clients, including municipal governments, financial institutions, and insurance companies, on issues ranging from questions about insurance coverage to notice-rights and due process violations.

ents, and vendors. That's not all. The downstream effect of the interruption is often significant. For example, if Jane's calendar was compromised and she fails to file that personal injury lawsuit until the statute of limitations runs, she might find herself on the wrong end of her previous-client's malpractice lawsuit.

The complex state, federal, and international regulatory framework of laws governing data privacy creates certain notice and disclosure requirements when a security or privacy breach occurs. Failing to follow these regulations may result in fines. In addition, regulations, such as the California Consumer Protection Act and the Illinois Personal Information Protection Act, provide a private right of action for a consumer against a business for disclosure of certain PII in a data breach. Outside of the regulatory context, a security or privacy breach can lead to litigation in which claimants assert breach of contract and tort causes of action.

Ransomware attacks often result in business interruption for multiple weeks. (In the first quarter of 2021, companies experienced an average of 23 days of downtime due to a Ransomware Attack. *https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound*.) During this downtime, a business may have no choice but to breach time-sensitive contractual obligation with its customers and vendors. To the extent an intentional act or omission of the business owner or its employee led to the security breach, negatively affected individuals may seek to recover damages. In addition to these concerns, Jane is rightfully worried about her business's reputation.

Whether Jane's business survives this event depends, in large part, on her organization's cybersecurity and cyber risk management strategy. What follows is a discussion of certain plans, actions, and options that every business should consider as part of a comprehensive cybersecurity and cyber risk management strategy. While each organization's approach may be different, according to its unique business profile and needs, the proper time to enact an effective risk management strategy is now—before a breach.

Practice Information & Privacy Hygiene

Various federal and state laws may require businesses to promptly notify customers if their PII has been compromised. Companies must respond quickly and credibly to a breach in order to minimize disruption and loss of business, and to avoid or mitigate legal liability. There is no such thing as perfect protection, so it is critical that a business implements effective and efficient protocols when a breach is discovered.

Information and Privacy Hygiene can generally be thought of as the protocols that you or your company implement to minimize exposure after a breach.

Things that should be considered include:

- Maintain appropriate internal processes and procedures
  - o Have an Incident Response Plan. An Incident Response Plan allows your organization to respond security and privacy breaches in a systemic manner. A proper plan helps organiza-

tions minimize the consequences of the breach while maximizing the chance of efficiently taking appropriate actions based on your specific business.

- Establish a Data Access Policy. Segregate your networks by limiting unnecessary access. The principle is simple: the fewer people who have access to PII, the less risk and the greater the chance of identifying how, when, and where a breach originated. Identify custodians of information and limit who has access to protected information. Also, do not retain protected information for any longer than necessary to conduct business.
- Implement a recurring training program focusing on identifying and avoiding cybersecurity risks. While cyber threats are ever evolving, a consistent risk is you or your employees inadvertently granting access to a threat actor by clicking on the wrong link or opening the wrong email.
- Require multi-factor identification for system access. Often your native operating system has all the functionality that you might need, but because several requests for the same password or multiple factor identification annoys the typical user, these features get turned off.
- Have an in-house or third-party IT professional ready to deploy options in the event of a breach and to ensure that your system's cybersecurity is sufficient to obtain cyber insurance coverage. Your IT professional should be able to conduct a vulnerability assessment, in other words, "a technical assessment designed to yield as many vulnerabilities as possible in an environment, along with severity and remediation priority information. Vulnerability assessments are appropriate when you need a prioritized list of everything that's wrong, where the goal is to fix as many things as possible as efficiently as possible." (Daniel Miessler, Information Security Assessment Types, (July 3, 2022, 7:39 PM), ***https://danielmiessler.com/study/security-assessment-types/***.) The IT professional should also be able to conduct a penetration test. Different from a vulnerability assessment, this type of test is more particularly aimed at "one or more specific goals[.]" *Id*.
- Minimize and limit access to third-party vendors.
  - Vet third-party vendors and limit their access to only the information necessary to conduct business. Regulators, like the Consumer Protection Bureau, can hold a company responsible for a third-party vendor privacy breach if the protected data obtained originated with the business.
- Commit everything to writing.
  - It's one thing to say that we train people; it's a different thing to show the manual that you base the training on.
  - The more that you can show your work and document your protocols, the better off you will be in the event of a breach.
  - A record will help ensure that your incident response team has a process for "creating, retaining, and transfer[ring] knowledge regarding incident handling within the organization." *Id*.
  - Ensure your vendor agreements state that the vendors will follow certain safety precautions and standards and describe what they may or may not do with the data.

Just as Jane's overhead includes a service to host her websites, so, too, should her overhead account for costs associated with maintaining cybersecurity and insuring against potential cyber liability.

A Primer on Cybersecurity Insurance Coverage

Businesses frequently address potential risk and liability through purchasing insurance coverage for general liability, directors' and officers' liability, property liability, and crime. Every business should consider the benefits and costs of adding cyber insurance to its risk management arsenal.

The cyber insurance market is unlike the other, more developed, insurance markets listed above. The relatively recent and ever evolving cyber risk and regulatory landscape has created a cyber insurance market with non-uniform policies. In addition, underwriting trends show continued increases of policy premiums and new entrants into the cyber market in response to an increased demand for this sort of coverage. Further complicating matters, because cyber insurance is a developing product, the language in cyber insurance policies is generally untested by courts. This uncertainty leads to risk for both insurers and insureds. The expense of cyber insurance and nature of the risk requires an organization that purchases a cyber policy to carefully evaluate its needs and confirm the scope of coverage while minimizing gaps in coverage.

A cyber incident can sink a company or its reputation, and the threat actors perpetrating these crimes know it.

Companies considering cyber insurance should:

- Identify insurers who offer the product best suited to an organization's needs.
- Evaluate the scope of coverage offered under insurance policies.
- Negotiate favorable terms and pricing.
- Complete the insurance application process to avoid potential misstatements and omissions.
- Identify and remove policy language that will likely lead to litigation and coverage denials.

The principal benefit of cyber insurance is that it sets a business' potential exposure in the event of a security or privacy breach. Breaches are often extremely costly. Potential first-party expenses include forensic investigation, legal costs, notifications, crisis response/ public relations, repairs and remediation, lost business income, fraud payments, and ransom payments. Potential third-party expenses include lawsuits and consumer claims, government inquiries and investigations, and contractual liabilities. Some carriers will also offer risk management services under their cyber

policy. These services may assist in cybersecurity assessments or audits, incident response plan assessments, and other systems testing.

While cyber policies differ, each typically includes a mixture of the following coverages:

- First-Party Coverages
  - o Cyber event management (notification/remediation) – covers the costs of notifying appropriate parties and effort needed to mitigate the damages in real-time.
  - o Business interruption – reimburses businesses for down time caused by the incident when the business would have otherwise been earning income.
  - o Data recovery – covers the costs of the restoring lost data.
  - o Cyber extortion & cyber-crime – while these coverages are different, both generally provide coverage in the event that a security breach or privacy breach has been manufactured by a bad actor with the criminal intent to force additional costs upon a business, whether that cost takes the form of a ransom demand or unlawful disclosure of PII. Note that some carriers exclude coverage for cyber-crime perpetrated by state actors.

Companies must respond quickly and credibly to a breach in order to minimize disruption and loss of business, and to avoid or mitigate legal liability.

- Third-Party Coverages
  - o Network security and/or privacy liability coverages – protects the insured against losses for the failure to protect a third party's PII or PHI.
  - o Media liability – protects the insured from liability arising out of the large-scale dissemination of information which might be libelous, or otherwise cast a third party in a false light.
  - o Technology E&O liability – this coverage can overlap or be similar to privacy liability coverage, however it is meant to protect the insured, not from malicious calculation, but from errors, omissions, negligence and failures in products—for example a tech company whose product has a glitch that results in liability.
  - o IP liability – protects an insured who might become a target for infringing upon another's intellectual property rights.

Assessing Cyber Risks and Coverage Needs

An entity's first step in selecting effective cyber coverage is assessing its cyber risk. Examples of questions that are relevant to the nature of a business's cyber risks include:

- Does a business rely on credit card payments from companies or processors that will impose fees in the event of a data breach?
- Does a business collect and store PII or PHI? If so, are the data elements involved sufficient to implicate notification and related expenses in the event of a breach?
- If a business stores valuable non-protected data, what costs are associated with restoring or destroying that information after a privacy breach?
- Does a business have cybersecurity vulnerabilities from insider threats?
- What is the risk that threat actors could successfully attack a business's system?

The best way for a business to conduct this analysis is through a cross-disciplinary approach involving its information technology, compliance, human resources, operations, and risk management departments. These departments should collaborate to determine the nature of the data that the business maintains, the legal obligations in the event of a data breach, the cost to recreate data, the business's security and data control programs, and previous threats.

Once a business understands its cyber risks, it should assess coverage needs. This starts with a review of an organization's existing insurance program to determine any gaps in coverage. Aside from the types of coverage, a business should consider the need for appropriate retroactive coverage for unknown breaches, retentions needed, appropriate limits and sub-limits, premium costs, and control in post-incident decision-making.

Applying for a Cyber Policy

After assessing cyber risks and coverage needs, a business may begin shopping and applying for coverage. A business applying for cyber insurance should expect to complete a detailed underwriting application designed to convey the nature of the business's risks to the prospective insurer. Responding fully and accurately to all information requested in an application is critical to avoiding potential coverage disputes. Businesses should take the application process as an opportunity to double check its risk assessment.

Before writing coverage, insurers may also require the applicant to implement certain risk-mitigation efforts, such as encryption, security audits, and enhanced security systems. Other insurers reduce the price of coverage for applicants that choose to implement these measures. Either way, these protections can only benefit a business in strengthening its cyber risk management strategy. By the time a business has reached the point of negotiating coverage it will likely have conducted several reviews of its system and taken steps to become more secure.

A prudent company should negotiate the broadest coverage possible to decrease the likelihood of coverage denial and litigation. Examples of broader coverage that may be available include coverage for the liability of third parties, such as vendors; all regulatory investigations, not just named agencies; unencrypted devices, like employees' personal devices; cyber-crimes by state actors; and data restoration costs that encompass replacing, upgrading, and maintaining previously breached systems.

Maintaining Your Cybersecurity and Cyber Coverage

As with all things in risk-management, assessing coverage is an iterative process. Companies should complete electronic source data and binding operational directive reviews on an annual basis. In addi-

tion, once a cyber policy is effective, a business should complete periodic assessments to maintain the best coverage while minimizing risk. Companies should periodically monitor and evaluate their coverage and confirm that it meets the changing risks relative to the marketplaces' offerings. The need for such monitoring is especially acute because more insurers continue to enter and change the cyber insurance market. Finally, a savvy business will periodically audit its documents and ensure compliance with its cyber policy's coverage conditions to minimize possible coverage disputes.

Evaluating Other Contracts and Agreements—Implement Burden Shifting

Companies often prevent, shift, and mitigate risk, including cyber risk, through contracts with business partners, contractors, and vendors. A prudent business should review its contracts and include defense, indemnity, hold harmless, and insurance provisions that address cyber risk. Here is an example of a specific contractual insurance requirement:

> During the Term and its own expense, Contractor will maintain the following insuance carriers rated A- or better by A.M. Best Company.
>
> **Cybersecurity and Privacy Insurance.** If Contractor will collect, store, process or otherwise access any data related to its customers. then Contractor will maintain network security and privacy liability insurance with coverage limits of not less than US $1,000,000 per claim, that includes coverage for: (A) Contractor's unauthorized disclosure of, or failure to properly handle, personal or other confidential data; and (B) financial loss, including any related defense expense, resulting from Contractor's wrongful acts.

A business should ensure that contractual provisions address necessary specific business risks and needs through detailed requirements addressing notice requirements, limits, retentions, sub-limits, refreshing limits, waiting periods, coverage parts, and insurance schedules.

Requiring vendors to notify your business and its insurer as soon as possible is advisable. Jane should not have to bear the burden of a breach that a party who she trusted, such as a vendor, allowed to fester through their silence. In practice, drafting such language is difficult. Often, the discovery of a breach does not immediately yield actionable information. It can take several days for anyone to obtain such information and ascertain the extent of the security or privacy breach. "It is important to strike a balance between the desire for transparency and the realities of [a] breach response to ensure that the notice customers receive is useful and actionable." (Kobus, Ted, Digital Assets and Data Management – Resilience and Perseverance, 2022 Data Security Incident Response Report (Baker Hostetler), at pg. 3.) Establishing a blanket rule requiring notice to your business within 24 hours of a suspected security or privacy breach is, nonetheless, advisable. If for no other reason, it at least ensures that your business should be on the list of parties to contact when a breach is discovered.

Quickly React to a Breach

Whether or not a business has cyber insurance, it should react to a cyber event by swiftly executing its Breach Response Plan.

Because Jane is a prudent businesswoman, she purchased a cyber insurance policy after completing the steps discussed above. So, what does she do now? First, she must report. Cyber policies are typically claims-made and reported policies—meaning the policy only covers incidents that occur in and are reported within strict specified periods. Thus, Jane must report the claim or potential claim even if she does not know the extent of the breach. Failing to do so may provide a valid basis for the insurer to deny or dispute coverage.

Jane should not fear notifying her cyber insurer. As an attorney, she appreciates the need to operate in an abundance of caution, especially in a field that has widely embraced and adopted network-based information storage. Likewise, her insurer should also appreciate her caution as prompt action typically mitigates damages caused by a breach.

After timely reporting the claim, Jane's insurer must act in accordance with the cyber policy's terms. Based on the coverage that Jane purchased, her insurer will acknowledge receipt of the claim and immediately take appropriate steps. according to the policy of insurance, to evaluate the situation, mitigate potential exposure, and restore her systems. To the extent necessary, Jane's insurer may retain coverage counsel, privacy counsel, a breach coach, and valuation/forensic accounting specialists to handle the loss. Jane must work closely with these vendors in accordance with her business's cyber policy.

Concluding Remarks—A Wide Net Full of Minnows Is Preferred to Targeting a Whale

While headlines focus on large-scale cyber-attacks, such as the Colonial Pipeline and SolarWinds breaches, threat actors do not discriminate—they target businesses of all sizes and in all sectors. The business and professional services industries, together, were the second most targeted industries by cyber threat-actors; only healthcare, including biotech and pharmaceutical companies, were more frequently targeted. *Id*. Still, the average ransom paid by businesses and professional services amounted to $342,370. *Id*., at 4. This amount is the lowest paid by all other sectors excepting government and education. Healthcare, financial services, hospitality, manufacturing and energy/technology companies all paid, on average, higher ransoms.

Rather than developing novel ways to attack newly hardened big-fish, threat actors increasingly target businesses lower on the food-chain with existing and tested software. Threat actors try to isolate small- and medium-sized entities from their sources of aid. In trying to keep their targets quiet, threat actors hope to repeat their attacks without diminishing returns. By vigorously protecting her business from and planning for a breach, Jane helps insulate her business, its customers, and its vendors from security and privacy breaches. All business owners should follow Jane's example and remain on-guard while working to employ and maintain robust cybersecurity and cyber risk management systems.