Chapter 12

Cyber Insurance

In May 2014, the Montana Department of Public Health and Human Services (DPHHS) announced one of the largest potential breaches of healthcare data reported to date. More than 1.3 million people's records may have been exposed—more than the population of the entire state, which had only a million residents at the time. A department server had been hacked in July 2013 and wasn't discovered until ten months later. According to the state's notification, the server may have contained names, addresses, birth dates, Social Security numbers (SSNs), as well as "information related to health assessments, diagnoses, treatment, health condition, prescriptions, insurance, and bank account numbers."[1]

Once the unauthorized access to the server was detected, the state's response was swift and effective—in large part because it had help. "We were the first state to have cyber insurance," said Lynne Pizzini, chief information security officer (CISO) of Montana. Pizzini, a 27-year veteran of the IT industry, founded the state's information security program (she became passionate about information security after a janitor unplugged her server one night to plug in a vaccum). In FY 2012, the state had added a $2 million breach response policy through a speciality insurer, Beazley.

The breach response insurance proved invaluable when the DPHHS incident occurred. "We immediately pulled the server off the network and contacted our insurance company," said Pizzini. "They immediately sent us a legal contact that met with us on a daily basis and developed the communications plan, based on requirements in all fifty states. We started having daily incident meetings with the Department of Health. [The attorney] flew out the next day after we notified the insurance company."[2] The insurer also connected the state with a forensics firm, which began the technical investigation.

Since the information on the server included personal information (as defined by state law), as well as protected health information, the clock was ticking with respect to notification. Montana's data breach law required notification "without unreasonable delay," and HIPAA had a 60-day notification requirement (beginning on the day of discovery).

Within ten days, the forensic investigation was complete—a quick turnaround for a forensics case, but still painfully slow for the state's management team. ("It was agonizing!" said Pizzini, of the wait.) Forensic investigators reportedly found no evidence that the data had actually been

1. Montana Department of Health and Human Services (DPHHS), "Notice Regarding DPHHS Computer Server," accessed January 19, 2018, http://web.archive.org/web/20150105200535/http://dphhs.mt.gov/Portals/85/Documents/ComputerServerNotice.pdf.

2. Lynne Pizzini, interview by the author, May 22, 2017.

accessed, but there was not enough evidence to rule it out. The state had to decide whether to notify the public.

Ultimately, said Pizzini, Governor Steve Bullock made the decision to notify the public "out of an abundance of caution." The state issued a press release describing the incident, along with a dedicated help line that individuals could contact between Monday and Friday, from 7 a.m. to 7 p.m. The insurer's breach response team "knew what frequently asked questions we should have answers to, because of the experience they had working with clients," explained Pizzini during our interview. "They set up a call center, an 800 number, and had people available to answer the phone with us. . . . It was immediately used. There's no way we could have had any of those things in a timely manner [without insurance], because we didn't have the contracts that provided those services."[3]

The Associated Press reported statements from key executives that were perfectly in line with the notification, illustrating a well-coordinated response. "There is no information, no indication, that the hackers really accessed any of this information or used it inappropriately," said Richard Opper, director of the DPHHS.[4]

Montana then faced the daunting challenge of mailing notification letters to 1.3 million people. "[The insurer] helped us with the notification," explained Pizzini. "We had seven different letters because of the data that was on that server." Included was an offer for credit monitoring. By late June, an approved notification letter template was sent to a mail processing center, along with names and addresses for delivery. On July 3, the mail processing center began sending letters to affected individuals, at a rate of 200,000 per day.[5]

The public relations impact was short lived, with a few news reports and relatively little attention given the number of affected people. There were no lawsuits. The state's policy covered the vast majority of forensics, legal, and notification costs. Just as with auto insurance, the state's premium for cyber insurance went up after the DPHHS breach, although Pizzini says it was "well worth it just to keep the insurance."

Cyber insurance had changed the game by the time Montana discovered the DPHHS incident in 2014. While many organizations struggled upon discovering a potential breach, trying to figure out what to do and how to handle the public relations fallout, those with access to breach response services found that they had an experienced team at their fingertips. The immediate support of a team of experts, as well as quick access to call centers, bulk mailing providers, and other important services, meant that Montana was able to respond quickly, meet legal requirements, and implement an effective crisis communications plan.

Pizzini is quick to point out that cyber insurance is not a substitute for preventative measures—although she says cyber insurance can help spur the development of good cyber-security programs. "You can't get it until you have a good program in place!" she says. "We've evolved because the requirements weren't as stringent back when we first got it. You have to have a firewall. You have to have intrusion detection. You have to have policies, security training. It's

---

3. Pizzini interview.

4. Lisa Baumann, "Montana to Notify 1.3 Million of Computer Hacking," Associated Press, July 2, 2014, https://insurancenewsnet.com/oarticle/Montana-to-notify-13-million-of-computer-hacking-a-525670#.XPcPZxZKipo.

5. NASCIO, "Are You Ready? Disruptive Change Is the New Norm" (NASCIO Mid Year 2015 Conference, Alexandria, VA, April 16–29, 2015), https://www.nascio.org/dnn/portals/17/2015MY/Cybersecurity%20Insurance.pdf (accessed January 19, 2018).

all of those things that are part of a good security program . . . which is understandable, because they don't want to have to pay for an incident."[6]

12.1 Growth of Cyber Insurance

At the end of 2017, insurers wrote an estimated $4.52 billion in global premiums for cyber insurance annually. Researchers estimated that volume could balloon to $17.55 billion in 2023.[7] According to Price Waterhouse Cooper, "[a]s recognition of cyber threats increases, take-up of cyber insurance in under-penetrated industries and countries continues to grow, and companies face demands to disclose whether they have cyber coverage (examples include the US Securities and Exchange Commission's disclosure guidance)."[8]

The growth of cyber insurance is driven by increasing costs, regulations, and media attention on data breaches. As organizations scramble to reduce their risk, they face two options: mitigate or transfer. Risk mitigation is an important part of the cybersecurity puzzle, but much like car accidents, bad things are bound to happen. Insurance allows you to transfer that residual risk to third parties, to protect your organization.

Cyber insurance is typically designed to transfer risks associated with loss of confidentiality or availability of data. Since the topic of this book is "data breaches," we will primarily focus on the risks associated with loss of confidentiality, although these often go hand-in-hand with operational impacts and outages.

12.2 Industry Challenges

As alluring as cyber insurance is, the industry is fraught with challenges, both for insurers and consumers. Cyber threats are constantly changing. Whereas once a "cyber" policy might need to primarily cover losses due to network outages or data exposure, today's high-risk threats include ransomware, cryptojacking, and more.

IT infrastructures are changing, too—and the risks change with them. The insurance industry's CRO Forum cited five factors that influence the threat landscape:[9]

- The cloud
- Shadow IT ("when business functions procure IT solutions without involving the IT department")

6. Pizzini interview.

7. "Global Cyber Security Insurance Market 2018," *Reuters*, May 16, 2018, https://www.reuters.com/brandfeatures/venture-capital/article?id=36676.

8. PwC, *Insurance 2020 & Beyond: Reaping the Dividends of Cyber Resilience* (London: PwC, 2015), https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.

9. CRO Forum, *Cyber Resilience: The Cyber Risk Challenge and the Role of Insurance* (Amsterdam, Netherlands: CRO Forum, December 2014), 7, https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf.

- Mobile and flexible working
- Bring Your Own Devices (BYOD)
- Internet of Things (e.g., smart buildings, wearable devices, appliances, etc.)

Finally, coverage options are not standardized and are often unclear. Cyber coverage can overlap with standard property and liability coverage, leading to questions about who is responsible for covering a loss—or whether anyone is responsible at all. "Policy wordings are currently inconsistent, with evidence of some clear cyber exclusions, some explicit inclusion . . . and many policies which are not explicit either way."[10] The details of coverage vary widely, with certain types lumped together under different names depending on the provider, and significant variation in the definitions of common terms such as "personal information."

12.3 Types of Coverage

Cyber insurance can include both first-party and third-party coverage. First-party coverage insures against losses related to damage that affects the insured organization itself, such as data destruction, lost revenue due to operational outages, and other impacts that directly affect the policyholder. Third-party coverage involves liability related to other parties as a result of a cybersecurity incident or data breach, such as consumers affected by exposure of their personal data, banks and card brands that are impacted by a payment card data breach, or regulatory bodies that assess fines.[11]

Common coverage options include:

- **Information Security and Privacy Liability** - Claims and damages payable due to parties as a result of a data breach or failure of computer security. This can even cover explicit violations of privacy or security-related laws, including liability for failure to notify affected parties in a timely manner following a breach. The costs of legal fees and other investigation expenses are often included.
- **Response/Remediation Services** - This covers costs associated with breach response. In some cases, the insurer will provide breach response services. Covered services may include:
  - Forensics services
  - Legal counsel
  - Crisis management
  - Call center services
  - Public relations

10. CRO Forum, *Cyber Resilience*.

11. "A Buyer's Guide to Cyber Insurance," Law360, October 23, 2013, https://www.law360.com/articles/480503/a-buyer-s-guide-to-cyber-insurance.

  - Notification
  - Credit monitoring/identity theft protection offers

In some cases, items from this list may be split out into separate coverage. Insurers may also provide proactive breach response training at no charge, such as tabletop exercises, training videos, and more.

- **Regulatory Defense and Penalties** - Costs related to regulatory action such as investigation, assessment, or penalties due to a violation of privacy or security regulations. For example, this might cover fines assessed by the Office for Civil Rights (OCR) due to HIPAA violations or the legal fees associated with appealing a penalty.
- **Payment Card Industry (PCI) Fines and Expenses** - Since PCI is a contractual requirement and not a regulation, associated fines and expenses are typically not covered under regulatory defense and penalties. Many insurance policies explicitly exclude contractual obligations. Organizations that process or store payment card data should consider obtaining PCI-specific coverage.
- **Network Interruption** - Lost revenue due to a cyber event, such as a denial-of-service attack on a retailer's website.
- **Media Liability** - Costs that the policyholder is required to pay as a result of copyright infringement, plagiarism, defamation, libel, or other negligent acts relating to publication of media.
- **Public Relations/Reputation Management** - Public relations and crisis communications costs associated with managing a negative publicity event. This typically includes the costs of responsive advertising via digital media, television, and print; social media campaigns; and image monitoring. In some cases, proactive reputation management plans and training are included.
- **Information Asset** - Expenses to restore, repair, or recreate data after corruption, destruction, or other loss.
- **Cyber Extortion** - Ransom payments and other fees associated with an extortion involving digital assets. This type of coverage typically covers the costs of retaining security professionals to help resolve the incident.
- **Cyber Terrorism** - Coverage for damages as a result of an act of cyber terrorism, typically as defined by the federal Terrorism Risk Insurance Act (TRIA). This means losses must exceed $5 million in aggregate and result from a "violent act or an act that is dangerous to human life, property or infrastructure" and is committed "as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion."[12] Terrorism (and war) are often explicitly excluded from coverage, unless a cyber terrorism endorsement is purchased.

12. Terrorism Risk Insurance Act §102(1), 15 U.S.C. §6701 note (2002); see also Alex Reger, *Terrorism Risk Insurance Program* (Research Report 2016-R-0208, Connecticut General Assembly, Office of Legislative Research, November 1, 2016), https://www.cga.ct.gov/2016/rpt/pdf/2016-R-0208.pdf.

- **Proactive Risk Management** - A relatively new development in cyber insurance is the integration of risk management tools and services, combined with cyber coverage. This can include security controls assessments, enterprise risk management assessments, response readiness evaluations, vulnerability scans, and other offerings—in addition to standard breach response services.

From Coffee to Cyber

I stood on the second floor of Lloyd's of London, leaning over the glass railing. Down below, men and women in suits and ties busily conversed in polished wooden booths (or "boxes," as they are called), with gray signs above that read "Advent," "Chaucer," "Beazley," and more. Here and there, small groups of professionals stood conversing. Tiny printers and copiers dotted the floor.

"Lloyd's started out as a coffeeshop in the seventeenth century," my guide explained to me. To attract shippers and merchants to his establishment, proprietor Edward Lloyd provided news about ships that arrived, departed, sank, and other status updates. Groups of customers sat in wooden boxes, drank coffee, and conversed. A sunken ship could be devastating to ship owners and merchants, who would lose not only the vessel but the very expensive cargo as well. Over time, frequenters of Lloyd's Coffee House banded together, and groups began to insure each other so that if a ship sank, many people would chip in to cover the losses. Eventually, Lloyd's of London was born.

In the center of the main floor was the *Lutine* bell, a recovered remnant from the sunken HMS *Lutine*. In 1779, the German economy was on the verge of a crash. The HMS *Lutine* was loaded with an estimated $1.2 million in gold (worth more than $130 million in 2017 U.S. dollars) and sent to Germany to support the banks. A storm struck, and the ship sank, along with its valuable cargo. The ship and its cargo were insured through Lloyd's, and amazingly, the Lloyd's syndicate paid the full cost of the enormous claim, within two weeks. "It was the *Lutine* that created Lloyd's reputation for paying valid claims—and for having the financial wherewithal to withstand a loss of such legendary proportions."[13]

In 1858, a recovery operation yielded the ship's bell, which was hung in the center of Lloyd's. The bell is rung to indicate important news: once for bad news (such as a sunken vessel) and twice for good news (such as a returning ship).

Today, brokers on the floor don't just plan for the breach of a vessel—they plan for data breaches, too. Lloyd's syndicates specialize in specialty insurance, insuring many unusual risks such as kidnapping, political unrest, war, and even famous body parts, such as Keith Richard's fingers. It was the perfect place to learn about a new and rapidly changing type of policy: "cyber" insurance.

12.4 Commercial Off-the-Shelf Breach Response

Cyber insurance has changed the game when it comes to data breach response—and not for the reasons that most people think. While cyber insurance has existed for two decades in one form

13. "HMS Lutine," *Lloyd's*,https://www.lloyds.com/about-lloyds/history/catastrophes-and-claims/hms-lutine.

or another, the common thread through all policies is financial coverage for claims or expenses due to a cyber event. Around 2009 a groundbreaking change occurred: Insurers began offering data breach *response services*. Instead of simply covering the costs, insurers provide access to their own response teams that support thousands of policyholders. This may include breach response professionals directly employed by the insurer, as well as forensic analysis, attorneys, and other specialists from third-party vendors.

Mike Donovan, the global head of technology, media and business services for Beazley Group, came up with the idea for breach response insurance in 2007. At the time, data breach regulations had picked up steam. There were notification laws in many states, and breaches were on the rise.

But few organizations had access to the specialists required to provide experienced advice regarding data breach investigations and response, such as attorneys who were familiar with data breach notification laws in all 50 states or forensic investigators who knew how to preserve and analyze volatile, nonvolatile, and network-based forensic evidence. Even organizations that could afford these services without insurance typically did not have the time or connections to build their own panels of providers that specialized in data breaches.

Donovan and his team recognized that many organizations were struggling with cybersecurity incident response. "To be able to develop [breach response] capability was not easy," he reflected in an exclusive interview. "This was particularly true in the midmarket space. It was almost impossible. You're trying to line up credit monitoring after you've had a large breach when you have no relationship with anyone who provides it, you have no idea what the right price should be and you have to get it set up in a week. You have to mail [notifications] and you have no idea who to hire and you have to get them out."[14]

Mishandled data breaches were—and still are—far more costly and expensive than a breach where the response is quick, efficient, and tightly managed. Often, consumer lawsuits, negative PR attention, and regulatory fines are the result of delayed notification or lack of effective crisis communications (as the case of Target illustrates; see Chapter 7, "Retailgeddon"). There are even times where a "breach" might not have been declared a breach at all if evidence had been properly preserved.

Donovan and his team realized that their clients needed quick access to services in the event of a breach—and that insurers were uniquely positioned to help. "With normal insurance, an event happens and you insure the outcome of that event," Donovan explained. "A traffic event happens and the insurer responds to whatever damage exists at that time. The insurer is not in a position to do anything as the accident is happening. In the cyber space, the loss was happening in a very different way. These were crisis events. They were happening in real time."

Instead, Donovan envisioned a different model. His team would essentially act as a clearinghouse, connecting their clients with seasoned experts, right when they needed help the most. "When a breach happened, we already had talent experts," he explained. "We had call centers. We had credit monitoring. We had everything they needed to respond in an effective manner. We could bring it to them immediately." His goal was to reduce the losses for everyone. "If the breach is handled well, the chance that they'll suffer reputational damage, lawsuits is much less."[15]

14. Mike Donovan, interview by the author, May 25, 2017.

15. Donovan interview.

Today, many insurers offer breach response services (as do law firms, credit bureaus, and cybersecurity companies). When a policyholder contacts the insurer with a suspected breach, a team member quickly responds and brings in third-party specialists such as legal counsel or forensic investigators as needed. The insurers maintain panels of service providers, including forensic analysts, data breach attorneys, call centers, PR firms, and other vendors that specialize in breach response and are available on short notice to assist. For small to midsized organizations or any entity that does not manage data breach crises on a day-to-day basis, the services of an experienced third-party breach response team can prove invaluable.

When breaches are handled effectively, the response and liability costs are greatly reduced, and damage is minimized. By providing policyholders with quick and easy access to experienced providers in a time of crisis, insurers can elevate the quality and speed of data breach response and thereby reduce losses. This is a win-win for both the insurer and the insured.

12.4.1 Assessing Breach Response Teams

When choosing an insurance policy, consider the insurer's role in your breach response process. Will you be leveraging response services provided by the insurer or an approved provider? If so, ask the following questions:

- **Ease of Contact** - How easy is it to contact your insurer? Do you have 24/7 availability, or more limited hours?
- **Responsiveness** - What can you expect for the response time? Some insurers may respond in minutes, whereas others may take days or weeks to process your request and assign providers. Responsiveness can make a big difference in the outcome of a data breach investigation, especially given that evidence can spoil at any moment.
- **Approved Providers** - How experienced are the vendors on the insurer's panel? Some insurers carefully vet their providers based on quality of work to make sure they're hiring experts. Others may select vendors based on favorable rates, market position, or other relationships.

  Even if your insurer's panel is excellent, you may prefer to work with a different legal counsel or forensic investigator with whom you have an existing relationship or whose name you received from a trusted source. "Selection of counsel continues to be a delicate issue with insureds," writes risk consultant Richard S. Betterley, "but as we frequently see in other new lines of coverage, carriers typically reserve the right to select, or at least approve, counsel."[16]

  Make sure to address the issue of provider selection during the procurement phase—not in the heat of the moment when a suspected breach occurs. Carefully review the list of approved service providers, and find out what it would take to use your own selected vendor. Consider asking to get your vendors preapproved so that in the event of a suspected breach, you can hit the ground running.

16. Richard R. Betterley, *Cyber/Privacy Insurance Market Survey: 2017* (Sterling, MA: BRC, 2017), https://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf.

12.4.2 Confidentiality Considerations

Be aware that when you purchase breach response coverage, you may be required to disclose ongoing details of the event with your insurance provider in order to receive coverage. The insurer is footing the bill, after all, and may have the right to review your service agreements, communications with providers, and reports. The vendors that you work with—including forensic investigators—may have contractual obligations to the insurer that require them to provide copies of your reports or other information about your case to the insurer.

As with any type of insurance, a negative event may affect your coverage and costs for future policies. For example, in the case of Sony Pictures Entertainment, when a breach occurred in 2011, the company made a $1.6 million claim against its policy with Hiscox. (Ironically, the details of Sony's insurance claims and negotiations were made public after its next major breach in 2014.) Steve Ragan of *CSO* magazine analyzed the leaked documents and determined that "due to exposures, as well as their $1.6 million claim, Hiscox didn't want to write a new policy, and thus declined to quote at renewal."[17]

12.5 How to Pick the Right Cyber Insurance

Cyber insurance isn't one-size-fits-all. A good policy can help you:

- Transfer risks to a third party
- Respond effectively to a breach
- Reduce the risk of a breach occurring in the first place

However, a policy that's not aligned with your risk profile or business needs will just be a waste of money. How do you choose the policy that's right for you? Here is a simple checklist:

Cyber Insurance Checklist

☑ Involve the Right People
☑ Inventory Your Sensitive Data
☑ Conduct a Risk Assessment
☑ Review Existing Coverage
☑ Obtain Quotes
☑ Review and Compare Quotes
☑ Research the Insurer
☑ Choose!

17. Steve Ragan, "Breach Insurance Might Not Cover Losses at Sony Pictures," CSO, December 15, 2014, http://www.csoonline.com/article/2859535/business-continuity/breach-insurance-might-not-cover-losses-at-sony-pictures.html.

Buying the Wrong Policy

"We had a really close call." It was Jenn, the office manager at a financial advising firm. Earlier that week, the firm had received a call from the bank notifying it that one of its money management computers had a virus. A staff member clicked on a link and accidentally downloaded malware, which was designed to steal banking credentials. Fortunately, the bank detected the suspicious activity—just in time.

The firm's executive team was spooked. "We manage a lot of money online," said Jenn. "We need insurance to cover a cash loss in case someone does break into one of our accounts." Within days, the firm's insurance agent sent over a quote. It was long and complex.

"Can you review it and tell us if it's the right coverage for us?" asked Jenn. The agent recommended the policy but the executive team wanted input from a cybersecurity professional.

After speaking with the agent, I reviewed the quote and concluded that it wasn't the right policy at all. The policy covered HIPAA violations, PCI violations, and breach response services appropriate for organizations bound by those regulations. However, the firm was not regulated by HIPAA and rarely handled credit card numbers.

After further research, we discovered that the firm's existing crime policy already covered the risk of money stolen from its online bank account. An in-depth discussion with its IT team revealed that the company had other critical risks that were not on the executive team's radar but that could be addressed by a different type of cyber insurance policy.

Time and time again, organizations ask their agents for "cyber" insurance, and the resulting quote is totally the wrong fit. Many organizations buy it anyway, not realizing until an issue comes up that they haven't covered their most critical risks.

Why does this occur? First, customers may not clearly communicate (or even understand) their coverage needs. Sometimes they just tell an agent they need "cyber" insurance and leave it at that.

On the flip side, agents often don't ask the right questions. They are not cybersecurity experts. Few agents have a strong understanding of the latest security threats or compliance requirements. Cyber policies themselves are so varied that it is hard for anyone to compare. The products are constantly evolving.

Know what risks you need to address, and get the right people involved in your cyber insurance selection process. That way, you can choose a policy that brings real value to your organization.

12.5.1 Involve the Right People

The first step in selecting your cyber insurance policy is to involve the right people, both inside and outside your organization. Cyber risk—and therefore cyber insurance—touches every part of your organization. Therefore, you need input from a variety of different functions during your decision-making process. Often, a cyber insurance policy is selected by management, finance, and legal, and then IT is told of its existence after the fact. This can result in insurance policy selections that don't reflect the true needs of the organization.

The exact persons you should involve will vary depending on your industry, size, and unique environment. Typically, it's wise to include people who handle the following business functions for you (either internal staff or outside service providers, depending on your organization):

- **Information Security** - If you have dedicated information security personnel, it's naturally a good idea to involve them so they can provide input regarding your key cybersecurity risks. Also, information security staff are responsible for implementing new security controls and tracking the changing threat landscape. You will need them to implement any technical requirements for maintaining coverage (such as mobile device encryption) and keep you updated if there are significant changes in your controls or the threat landscape that would require you to modify your coverage. Finally, information security staff are normally tasked with responding to potential data breaches, and so they need to be aware of insurance triggers and understand how and when to hand off to insurers and third-party service providers.
- **IT** - Your system administrators, help desk providers, and network engineers should have an intimate understanding of both the strengths and weaknesses of your network infrastructure. Much like information security staff, they may be involved in implementation of any technical requirements and have firsthand knowledge of changes to your IT infrastructure that would impact your risks. When a data breach occurs, your IT staff are often the first ones to see the signs, and they need to understand how to recognize indications of a breach and what information needs to be preserved and communicated in order to most effectively leverage your insurance policy.
- **Legal** - Your legal counsel will provide input on any risks that stem from contractual or regulatory requirements, such as PCI, state or federal breach notification or security laws, and more. While it's always wise to have your general counsel involved, it's also a smart idea to consult with a specialist attorney who has experience working with security and breach notification laws in all 50 states, and any specific industry or geographical region that's relevant to you.
- **Finance** - Your finance department can help you budget for cyber insurance, plan for payment of deductibles, and provide input on a cost/benefit analysis of your cyber insurance quotes. In addition, many cybersecurity risks relate directly to data that finance departments create, transmit, store, or process, including banking information, tax returns, employee SSNs, online banking credentials, and more.
- **Risk Management** - Your risk management personnel can help you prioritize risks, coordinate your risk assessment process, and define your coverage needs.
- **Human Resources** - Your HR department can help you evaluate and manage risks associated with theft of employee data (such as SSNs and W2s), insider attacks, and more. HR staff are often tapped with managing employee communications in the event of a breach, in order to ensure that employees have clear instructions and know how to respond to outside inquiries.
- **Public Relations** - Services such as crisis communications and reputation defense, often provided as part of a cyber insurance policy, naturally fall into your PR team's area of

expertise. Your PR team can help you vet insurance panel providers and evaluate your coverage needs.

- **Executive Team** - Typically the executive team has the bird's eye view of your organization and can oversee the cyber insurance selection process.
- **Board of Directors** - Ultimately, your board of directors should sign off on whatever policy you choose. Insurance is about transferring risk, and your board (or equivalent) should have the opportunity to understand and provide input on coverage choices, particularly when significant residual risk remains.
- **Insurance Agent** - You should always work through an experienced insurance agent who will review the policy in detail and advise you regarding coverage options.
- **Cybersecurity Specialist** - When it comes to cyber coverage, having an agent review your quotes is not enough. Use the buddy system when you buy cyber insurance. It is worth it to bring in an experienced cybersecurity professional who will work hand-in-hand with your agent to evaluate your risk, define your requirements, and review your quotes in detail. That way, you can make sure that the policy's coverage is truly in line with your organization's needs.

This is not to say that every person (or group) in this list should have an equal vote on your cyber insurance policy selection. Rather, the decision-making process should be designed to take input from all of these areas (and more, as needed) in order to accurately assess the organization's risk profile and evaluate the effectiveness of the proposed policy. Taking input from a wide field will help ensure that you are addressing cyber risks organization-wide, and it will also help you to obtain buy-in from the key stakeholders who will later be tasked with integrating and leveraging your cyber policy.

12.5.2 Inventory Your Sensitive Data

When you buy home insurance, it's wise to make an inventory of your property so that you know how much insurance to buy and what type of coverage you need. If you do need to make a claim, having the list readily available helps to expedite the process.[18]

Similarly, when you shop for cyber insurance, you should take an inventory of your data for much the same reasons. Refer to Chapter 2, "Hazardous Material," for guidance on taking an inventory of your data.

12.5.3 Conduct a Risk Assessment

Cyber insurance enables you to transfer risks to a third party. In order to pick the right insurance policy, you first need to enumerate and prioritize your risks. Too many organizations choose insurance coverage based on an executive's gut instinct about risk, rather than taking a methodical approach. Cyber insurance isn't cheap! Conducting a formal risk assessment will help ensure that your investment in cyber insurance is effectively spent.

---

18. "Home Inventory," Farmers.com, accessed January 19, 2018, https://www.farmers.com/inner-circle/home-tool-kit/how-to-create-a-home-inventory.

If you have sensitive information (and who doesn't?) chances are you should be routinely conducting risk assessments anyway, as per HIPAA, PCI, NIST Cybersecurity Framework guidelines. A word of caution, however: Many risk assessments are based on a subset of your network. For example, a HIPAA risk assessment may focus only on risks pertaining to ePHI. When you select cyber insurance, make sure you are basing your decisions on an enterprise-wide risk assessment.

Many people confuse risk assessments with controls assessments. These are not the same thing. A controls assessment is essentially a comparison of your existing controls with a known checklist, such as ISO 27001 or the NIST Cybersecurity Framework. You receive a report indicating controls in place and gaps.

In comparison, the NIST "Guide for Conducting Risk Assessments" (SP 800-30) states that "the purpose of a risk assessment is to inform decision makers and support risk responses by identifying: (i) relevant threats to organizations or threats directed through organizations against other organizations; (ii) vulnerabilities both internal and external to organizations; (iii) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring)."[19]

There are other effective models for assessing and communicating risk. For example, at Los Alamos National Laboratories, the security team uses an "attack tree" model. Threats and vulnerabilities are documented as leaves on a tree that interconnect, and the overall risk for a scenario is calculated based on the aggregate risk from all of the leaves. This model allows the team to evaluate the risk of the system as a whole, rather than individual parts in isolation.[20]

Once you have conducted a risk assessment, you can develop a risk management plan. A three- to five- year plan is common (you will want to update it at least annually in response to changes in your environment and the threat landscape). For each risk, determine whether you can mitigate or eradicate the risk. Some risks can be reduced or even eliminated with relatively little effort. Others cannot be addressed without a very large investment. Every organization has limited resources, and so there is a cost-benefit tradeoff to addressing risks. The organization will need to accept some residual risk.

The risks that the organization cannot eliminate but does not want to accept are prime candididates for *transfer* via insurance.

12.5.4 Review Your Existing Coverage

Before you reach out for quotes, make sure to review your existing coverage. Some cyber-related risks may be covered under your existing insurance. For example, commercial crime policies typically provide coverage for direct losses incurred by the policyholder as a result of malicious activity by third parties. So, if hackers break into your bank account and transfer $10,000 out,

---

19. National Institute of Standards and Technology (NIST), *Guide for Conducting Risk Assessments: Information Security*, Special Pub. 800–30, rev. 1 (Washington, DC: NIST, September 2012), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

20. Steven G. Howard, "Risk Based Information Security Model," Los Alamos National Laboratory, *National Laboratory Information Technology Conference (NLIT)*, June 15, 2011, https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-11-03062.

your commercial crime policy may well cover your cash loss. On the other hand, if the hackers also steal your employees' SSNs and open credit cards in their names, your crime policy would not cover your liability for any ensuing lawsuits or damages incurred by the employees or other third parties.

There are other areas where cyber-related risks *may* be covered by your existing insurance. "If there's a cyber attack that causes tangible damage to property, it could be covered under your property policy," said Kevin Kalinich, global practice leader for Aon Risk Solutions. "If there's an attack that causes tangible damage to a third party, your general liability policy could cover it."[21]

Once you identify your high-risk scenarios, review your existing policies to see if you already have insurance. Overlapping insurance policies mean that you're paying twice for the same coverage. Also, in the event that both policies are triggered, you could be faced with dueling insurers, which might slow down the process.

That said, tread carefully. There is often ambiguity in the ways that standard insurance policies apply to electronic data and breaches, which can lead to disputes between the policyholder and the insurance company. For example, in the case of *State Auto Property & Casualty Insurance Co. v. Midwest Computers* the defendant had insurance that covered "[p]hysical injury to tangible property." The court ruled that "[a]lone, computer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property." However, the coverage also included "[l]oss of use of tangible property that is not physically injured" and customers who had lost the *use* of their computers. Therefore, the court also stated that "[b]ecause a computer clearly is tangible property, an alleged loss of use of computers constitutes 'property damage' within the meaning of plaintiff's policy."[22]

Commercial general liability policies may provide some coverage for losses related to data breaches. For example, in 2013, two patients of Glen Falls Hospital discovered that their medical records turned up as the first result in a Google search for their respective names. Glen Falls had contracted a service provider, Portal Healthcare Solutions, LLC, to manage and store electronic patient health records. The patients initiated a class-action lawsuit. Portal attempted to trigger the company's commercial general liability insurance (provided by Travelers) to pay for the lawsuit, since it included coverage for "personal and advertising injury."[23] Travelers refused, arguing that "there was no 'personal injury' or 'publication' as defined by the policies because release of the records was not intentional and they were not viewed by a third party."

The federal appeals court in Virginia ruled against Travelers, stating that an unintentional publication is still publication. The court also said the definition of publication does not hinge on third-party access. Therefore, Travelers was required to cover Portal's legal defense costs

---

21. "Where Cyber Insurance Underwriting Stands Today," *Insurance Journal*, June 12, 2015, http://www.insurancejournal.com/news/national/2015/06/12/371591.htm.

22. American Online, Inc. v. St. Paul Mercury Insurance Co., 207 F. Supp. 2d 459, 470 (E.D. Va. 2002) (quoting State Auto Property & Casualty Insurance Co. v. Midwest Computers & More, 147 F. Supp. 2d 1113 (W.D. Okla. 2001), http://law.justia.com/cases/federal/district-courts/FSupp2/207/459/2346018.

23. Andrew G. Simpson, "Federal Court Rules CGL Insurance Covers Data Breach," *Insurance Journal*, April 12, 2016, http://www.insurancejournal.com/news/national/2016/04/12/404881.htm.

for the class-action lawsuit (since the commercial general liability [CGL] policy did not cover liability to third parties, so any resulting settlement or fines would be Portal's responsibility).

"What makes the decision important . . . is that they may have some data breach coverage that they didn't know they had," commented tech writer John P. Mello Jr., upon the announcement of the appeals court ruling in 2016.[24]

On the flip side, when the Sony Playstation network was hacked in 2011 and 77 million users' personal information was stolen, the company attempted to leverage the personal and advertising injury coverage in its CGL policy—and ultimately lost a battle with its insurer, Zurich American Insurance Co. "New York Supreme Court Justice Jeffrey K. Oing issued a bench ruling that the policy did not cover breach costs because the provision only covered confidential material published directly by Sony, not by the hackers who stole the information."[25]

Confused? You're not alone. "[S]everal courts had struggled with the definition of 'publication' . . . in recent years, with differing results," writes Jana Landon, data management attorney at Stevens & Young.[26]

As the cyber insurance industry matures, insurers have moved to explicitly exclude data breach and cyber-related coverage from CGL policies. "[U]nsurprisingly, given the confusion in the courts over these issues and the rapid uptick in third-party external hacking incidents, these standard CGL policies have now been updated to provide the insureds with further clarification," writes Landon. "For example, CGL policies now include the 2014 ISO form 'Access or Disclosure of Confidential or Personal Information Exclusion.' This exclusion expressly limits [Personal and Advertising Injury Liability Coverage] and excludes accessing or disclosure of, among other things, 'patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information.' In other words, most of the information that is compromised during data breaches."[27]

If you have an older policy, it may include broader coverage for data breaches and related expenses than newer policies. However, if there's any ambiguity whatsoever, don't count on it.

You want your cyber insurance policies to be "harmonized" with your existing insurance. Understand which of your high-risk scenarios are—and are not—covered by your existing policies. Try to find coverage that will minimize overlaps while ensuring that your needs are met. Consider purchasing cyber insurance from the same companies that underwrite your CGL and/or property insurance, to minimize the risk of conflicts in the event that multiple policies are triggered by an event.

---

24. John P. Mello Jr., "Insurance Industry Buzzes Over Data Breach Ruling," *TechNewsWorld*, April 21, 2016, http://www.technewsworld.com/story/83403.html.

25. Latham & Watkins, "Cyber Insurance: A Last Line of Defense When Technology Fails," (Client Alert White Paper No. 1675, April 15, 2014), 7, https://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage.

26. Jana Landon, "Where Does Sony Settlement Leave CGL Insurance for Data Breaches?" *Legal Intelligencer*, May 13, 2015, https://www.law.com/thelegalintelligencer/almID/1202726345560/where-does-sony-settlement-leave-cgl-insurance-for-data-breaches.

27. Landon, "Sony Settlement."

Cyber Insurance Towers

At Lloyd's of London, my guide and I stood on the balcony, watching the tiny insurance brokers negotiate on the floor below. For small or midsized organizations, purchasing insurance is a fairly straightforward process: You talk with your broker, obtain quotes, and pick one. Large organizations, such as the retailer Target, need hundreds of millions of dollars in cyber insurance. Few, if any, insurers will provide that amount of cyber insurance all at once. Instead, the organization must build a "tower" of cyber insurance, made up of many layers.

When building a cyber insurance tower, one of the challenges is getting the upper layers of the policy to match the terms of the primary layer. This can involve coordinating with dozens of different underwriters. Ryan Gibney, assistant vice president at insurance brokerage firm Lockton Companies, shared that he was working with one "new-to-the-market" client that sought a $200 million tower. To build the tower, he was coordinating with 27 U.S. insurers, 9 in London, and 9 more in Bermuda. "So, we're speaking with 45 different underwriters with 45 different appetites in order to meet the capacity."[28]

"It's a lot easier to build a tower when you have everybody in the same room," said my guide. Sure, brokers can—and do—negotiate complex policies via phone and email. But as we watched, we could see brokers gather and move from box to box at Lloyd's. "A broker gets one insurer—say, Bob from Beazley—to underwrite the first $5 million. Then, he might go over to Sue from ACE and say, 'Hey, you know Bob, who you had lunch with yesterday? He's underwriting the first $5 million. Would you like to get the next $10 million?' It's easier to get things done when you can talk face to face. A lot happens right here in this room."

12.5.5 Obtain Quotes

Once you've identified your high-risk scenarios and understand your existing coverage, you're ready to get quotes. The process will vary depending on the type and amount of coverage you're seeking. Before you begin, take the time to define the coverage you seek in writing. This way everyone will be on the same page. Get input from both your insurance agent and a qualified cybersecurity professional.

Typically, you'll be asked to fill out an application designed to assess your needs and level of risk. This will include questions about the volume and type of data your organization stores, what policies you have in place (and whether you follow them), access control, backups, monitoring systems, and more.

As data breaches continue to proliferate, more organizations are seeking high-dollar coverage—and insurers are vetting them more carefully. "[U]nderwriters have begun asking more thoughtful questions," said Thomas Reagan, the cyber practice leader for Marsh insurance brokers. He added that underwriters are vetting applicants' risk management programs and asking specific questions about whether the applicants leverage risk management technologies such as encryption, chip-and-PIN cards, and tokenization. "Underwriters are just

28. Erin Ayers, "Higher and Higher: Cyber Insurance Towers Take Careful Construction," *Advisen*, September 24, 2015, http://www.advisenltd.com/2015/09/24/higher-and-higher-cyber-insurance-towers-take-careful-construction.

another example of how organizations have to tell their story about their cyber risk management process."[29]

It's very important to be accurate in your application. If your cybersecurity controls and risks are substantially different than what you state in your application, then your insurer may be justified in claiming that you have concealed or misrepresented material facts, and deny a claim accordingly. Insurers can also require audits of your cybersecurity infrastructure to assess and verify your risk profile.

In the case of Cottage Health System in southern California, a routine security audit turned into a nightmare when auditors discovered that 11,000 patient records were exposed on an Internet-facing server managed by a third-party vendor, inSync. Cottage's insurer, Columbia Casualty Company, denied the healthcare provider's claims, stating that Cottage "provided false responses" to a "Risk Control Self Assessment" that the company completed as part of the application process. The questions and Cottage's responses included:[30]

> *4.* Do you check for security patches to your systems at least weekly and implement them within 30 days? *Yes*
>
> *5.* Do you replace factory default settings to ensure your information security systems are securely configured? *Yes*
>
> *6.* Do you re-assess your exposure to information security and privacy threats at least yearly, and enhance your risk controls in response to changes? *Yes*
>
> *11.* Do you outsource your information security management to a qualified firm specializing in security or have staff responsible for and trained in information security? *Yes*
>
> 12. Whenever you entrust sensitive information to 3rd parities do you . . .
>
> *a.* contractually require all such 3rd parties to protect this information with safeguards at least as good as your own? *Yes*
>
> *b.* perform due diligence on each such 3rd party to ensure that their safeguards for protecting sensitive information meet your standards (e.g., conduct security/privacy audits or review findings of independent security/privacy auditors)[?] *Yes*
>
> *c.* Audit all such 3rd parities [*sic*] at least once per year to ensure that they continuously satisfy your standards for safeguarding sensitive information? *Yes*
>
> *d.* Require them to either have sufficient liquid assets or maintain enough insurance to cover their liability arising from a breach of privacy or confidentiality[?] *Yes*
>
> *13.* Do you have a way to detect unauthorized access or attempts to access sensitive information? *Yes*
>
> 23. Do you control and track all changes to your network to ensure it remains secure? *Yes*

29. Ayers, "Higher and Higher."

30. Columbia Casualty Co. v. Cottage Health System, No. 2:16-cv-3759 (C.D. Cal. 2016), https://www.insideprivacy.com/wp-content/uploads/sites/6/2016/06/CNA-v-Cottage-Health-2016-complaint.pdf.

Columbia argued that these were "material misrepresentations and/or omissions of fact and that, consequently, Columbia is entitled to rescind the policy as void *ab initio*."[31] Ultimately, the case was dismissed for a different reason: because the policy required that the parties first attempt to resolve matters using alternative dispute resolution methods before turning to the courts.[32]

12.5.6 Review and Compare Quotes

Now, the fun part! Once you receive quotes from insurers, you can begin reviewing and comparing them. You may want to start by doing a high-level review of all the quotes that you receive and then, once you've narrowed it down, conduct a detailed examination of your top contenders. Make sure that both your insurance agent and your cybersecurity specialist review your quotes in detail. Then, involve key stakeholders within your organization when making the final decision.

12.5.6.1 Types of Coverage

Remember, you're rarely comparing apples to apples when reviewing cyber insurance policies. Sometimes it can feel like you're comparing apples to octopuses! What one underwriter calls "notification expenses" may mean something completely different in another policy.

For example, one cyber insurance policy covered "privacy notification expenses" in the event of a breach. However, the policy included "credit monitoring or other similar services" in the definition of privacy notification expenses. The sublimit for the "privacy notification expenses" was comparable to that of similarly named coverage offered by other insurers, but the other insurers separated credit monitoring into a different category. Given that credit monitoring is very expensive compared to simple notification costs, in the event of a breach the costs would have quickly exceeded the sublimit for privacy notification expenses.

12.5.6.2 Triggers

In order for you to receive payment or services under a cyber insurance policy, the policy must first be *triggered*. What is a trigger, in this context? According to the International Risk Management Institute, Inc. (IRMI), a *coverage trigger* is the "event that must occur before a particular liability policy applies to a given loss."[33]

---

31. *Columbia Casualty Co. v. Cottage Health System*.

32. Joe Van Acker, "Insurer's Failure to Mediate Kills Its $4M Data Breach Claims," Law360, July 20, 2015, https://www.law360.com/articles/680863/insurer-s-failure-to-mediate-kills-its-4m-data-breach-claims.

33. International Risk Management Institute (IRMI), "Coverage Trigger," accessed January 20, 2018, https://www.irmi.com/online/insurance-glossary/terms/c/coverage-trigger.aspx.

Pay careful attention to what types of events do—and don't—trigger your policy. For example, many cyber policies are not triggered until a formal lawsuit or request for monetary damages is filed. That means that any legal fees, fines, or work performed in response to government investigations or regulatory action may not be covered. The Cybersecurity by Chubb policy defines "claim" as:[34]

> A. any of the following:
>
> – 1. a written demand or written request for monetary damages or non-monetary relief;
>
> – 2. a written demand for arbitration;
>
> – 3. a civil proceeding commenced by the service of a complaint or similar pleading; or
>
> – 4. a criminal proceeding commenced by the service of an indictment,
>
> against an Insured for an Injury, including any appeal therefrom; or
>
> B. a written request received by an Insured to toll or waive a statute of limitations relating to a potential Claim described in paragraph A. above.

As you can see, a government investigation probably would not trigger coverage. Furthermore, even if a lawsuit were eventually filed, the policy specifically does not cover any expenses incurred prior to the time that an event meets the definition of a claim.

Attorney Steve Raptis of Manatt, Phelps & Phillipps LLP specializes in insurance advice and disputes. He recommends "[s]eeking trigger language that focuses on the insured's failure to protect confidential information, regardless of the cause (e.g., 'any failure to protect'), rather than language requiring an intentional breach."[35]

12.5.6.3 Retentions

Check the deductible and/or retention amounts on your policies carefully. Most people are familiar with deductibles since they are very common in car and health insurance. Your insurer is responsible for each claim, and the deductible is the monetary amount that you are responsible for.

A self-insured retention (SIR) is an amount that you are required to pay before one of your insurance policies kicks in. For example, in the case of Target, which reportedly was self-insured for the first $10 million of cyber coverage, the insurer would not get involved at all until the SIR was met.

---

34. "Cybersecurity by Chubb," Chubb.com, accessed January 20, 2018, https://web.archive.org/web/20180712175705/http://www.chubb.com/businesses/csi/chubb10308.pdf.

35. Steve Raptis, "Analyzing Cyber Risk Coverage," *Risk & Insurance*, March 13, 2015, http://riskandinsurance.com/analyzing-cyber-risk-coverage.

12.5.6.4 Covered Expenses

Make sure you understand exactly what expenses are covered in the event of a breach. For example, an AIG CyberEdge policy defines "loss" as specific "reasonable and necessary expenses and costs" incurred "*within one year of the discovery*" of a qualifying event, including coverage for forensics investigations, public relations, crisis management, notification, identity theft services, and more. The timing cutoff is buried in the definition itself and has huge implications for coverage, especially since data breach lawsuits can drag on for years. Also, the definition of "loss" explicitly excludes "internal charges"—meaning you may be better off hiring outside consultants whenever possible as opposed to conducting work in-house.[36]

A very common limitation, as expressed in a Beazley breach response policy, is that cyber insurance may cover "actual, reasonable and necessary costs and expenses incurred . . . to restore a Data Asset from back-ups or from originals or to gather, assemble and recollect such Data Asset from other sources to the level or condition in which it existed immediately prior to its alteration, corruption, destruction." It will not cover costs to "update, replace . . . or enhance a Data Asset or Computer System to a level beyond that which existed prior to the alteration . . . or damage of such Data Asset."[37]

12.5.6.5 Timing

Often, data breaches are discovered months or even years after the event actually took place—such as the Yahoo breaches publicized in 2016, which actually first occurred in 2013 and 2014. However, many cyber insurance policies will cover losses or claims due to breaches that occur only after the policy inception date or a "retroactive date" negotiated with the policyholder. Furthermore, the event typically must be discovered and reported to the underwriter during the period that the policy is in effect.

That means if a data breach occurred three years ago, before your insurance coverage took effect, but you discovered it today, your current cyber insurance might not cover the breach. Furthermore, if you switch insurers and later discover that a breach occurred while you had your previous policy, but you didn't detect or report it in time, you might not be covered.

What if a breach is ongoing, such as in the case of TJ Maxx, where hackers were accessing the company's network for a year and a half (see Chapter 6, "Payment Card Breaches")? Some insurers have specifically addressed these cases. For example, one Beazley Breach Response policy specifically states that "[a] series of continuing Security Breaches, related or repeated Security Breaches, or multiple Security Breaches resulting from a continuing failure of Computer Security, shall be considered a single Security Breach and be deemed to have occurred at the time of the first such Security Breach."[38]

Make sure to push the retroactive date as far back as you reasonably can, given your resources and coverage options. Also, be sure to understand the reporting requirements and

---

36. AIG CyberEdge, Security Failure/Privacy Event Management Insurance, December, 2013 (insurance policy, on file with author).

37. Beazley, *Beazley Financial Institutions and Breach Response Services Policy* (Report, Beazley, April 2014), 35, https://www.beazley.com/documents/Wordings/beazley-financial-institutions-and-breach-response-services-uk.pdf.

38. Beazley, *AFB Media Tech* (Report F00437, Beazley, September 2014), https://www.beazley.com/documents/TMB/Media%20Tech/MediaTechPolicy_SurplusLines_F00437092014ed.pdf.

have a strong detection program in place, so that you don't accidentally miss a reporting window and lose coverage.

12.5.6.6 Limits

Make sure that the limits of your insurance are in line with the volume and sensitivity of the data that you retain. When Anthem health insurance announced in 2015 that it had been hacked (see Chapter 9, "Health Data Breaches"), one of the most shocking aspects of the case was that it quickly smashed through the limits of its $100 million cyber insurance tower. Anthem's CEO, Joseph Swedish, confirmed that personal information of 78.8 million people had been exposed, including names, birthdates, medical IDs, SSNs, and more.

One hundred million dollars may seem like a lot of coverage—but not when the personal records of nearly *80 million* people are affected. "[T]his amount will not even be enough to cover the cost of postage, let alone cover damages due to the data breach," reported Presidio Insurance Solutions.[39] "And Anthem will have to spend millions more to fix its security problems and rebuild its reputation."

According to the *Insurance Insider*, Anthem's cyber insurance tower was built with Lexington (an AIG member) as the primary insurer, followed by eight upper layers, as illustrated in Figure 12-1. Note that these details are based on an anonymous source and have not been publicly confirmed by Anthem.

The total coverage limitation of a policy is important, of course, but pay attention to the sublimits as well. These are limitations for specific types of coverage within the policy. As illustrated earlier by the "privacy notification expenses" coverage, sublimits can have a big impact on the value of your policy.

There is a wide variation in the estimated cost of a breach per record, which adds to the challenge of calculating the potential costs of a breach (and thereby the appropriate insurance coverage, limits, and sublimits). According to the Ponemon Institute, the average per-capita cost of a breach in 2015 for U.S. citizens was $217. The same year, Verizon reported that the average per-capita cost of a breach was only 58 cents. That's a pretty huge difference, especially when you're calculating potential costs for almost 80 million people!

Some policies provide sublimits that are not tied to a specific dollar amount. For example, notification may be limited to 1 million individuals, or the call center services may be limited to 20,000 calls per day. These types of limits are less risky for the policyholder because they do not require it to translate the number of affected individuals into a specific dollar limit, which may fluctuate as breach response best practices, requirements, and services change.

Appropriate limits for your organization will necessarily depend, in part, on the sensitivity of the data that you hold, the potential for lawsuits, fines and long-term ("chronic") conflicts, and your risk appetite. Refer to the inventory of data that you created for your organization, and consider the costs of notification, credit monitoring, and other potential compensation for potential affected persons. Research fines or penalties for organizations that hold sensitive information that is similar to yours, such as medical files or payment card data. Make sure

39. Presidio Insurance Solutions, "What the Anthem Data Breach Means for Malpractice Insurance", http://www.presidioinsurance.com/news/anthem-data-breach (accessed January 20, 2018).

Figure 12-1. Illustration of Anthem's cyber insurance tower, based on unofficial details. Source: Adam McNestrie and Jenny Messenger, "Anthem Breach Could Exhaust $100mn Cyber Programme," *Insurance Insider*, February 16, 2015, https://web.archive.org/web/20150219100116/http://www.insuranceinsider.com/-1253434/10.

that you take into account all information that you hold, including archived data and employee records. Above all, remember that data is hazardous material, as Chapter 2 discusses.

As you compare the costs of various insurance policies, consider whether there is data that you can destroy, so that you don't have to wonder what it will cost in the event that is it exposed.

12.5.6.7 Exclusions

Cyber policies normally contain a laundry list of exclusions, which removes the insurer's obligation to provide coverage in certain scenarios. Many of these are straightforward and understandable, such as exclusions that explicitly carve out the insurer's obligation to cover

claims due to intentional crimes committed by the policyholder. However, there are some exclusions that dramatically change the value of your policy.

As an example, let's analyze the P. F. Chang's payment card data breach and subsequent insurance lawsuits, which hinged upon an exclusion for contractual obligations.

Contractual Obligations Exclusions

P. F. Chang's China Bistro is an Asian-style restaurant chain that processes more than 6 million payment cards each year. In 2014, P. F. Chang's purchased a Cybersecurity by Chubb policy through Federal Insurance Company ("Federal"), which was advertised as "a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world," including coverage for "direct loss, legal liability, and consequential loss resulting from cyber security breaches."[40] The owners paid an annual premium of $134,052 for the coverage.

On June 10, 2014, investigative reporter Brian Krebs broke the news that P. F. Chang's had suffered a major credit card breach. "On June 9, thousands of newly-stolen credit and debit cards went up for sale on rescator[dot]so, an underground store," reported Krebs. "Several banks contacted by KrebsOnSecurity said they acquired from this new batch multiple cards that were previously issued to customers, and found that all had been used at P. F. Chang's locations between the beginning of March 2014 and May 19, 2014."[41] Two days later, P. F. Chang's released a statement confirming the breach. Investigators later determined that 66,000 payment card numbers had been compromised.

P. F. Chang's immediately notified its insurer, Federal, which covered approximately $1.7 million in costs for forensic investigators and litigation defense stemming from lawsuits filed by customers and one issuing bank. In March 2015, P. F. Chang's also requested coverage for $1.9 million in fines and penalties assessed by Mastercard. The card brand imposed fees on P. F. Chang's payment processor, BAMS, which in turn sent the following letter to P. F. Chang's:[42]

> MasterCard's investigation concerning the account data compromise event involving [Chang's] is now complete. [BAMS] has been notified by MasterCard that a case management fee and Account Data Compromise (ADC) Operational Reimbursement and Fraud Recovery (ORFR) are being assessed against [BAMS] as a result of the data compromise. In accordance with your [Master Services Agreement] you are obligated to reimburse [BAMS] for the following assessments:
>
> - $ 50,000.00—Case Management Fee
> - $ 163,122.72—ADC Operational Reimbursement
> - $1,716,798.85—ADC Fraud Recovery 2
>
> $1,929,921.57

40. P. F. Chang's China Bistro, Inc. v. Federal Insurance Co., No. CV-15-01322, 1 (D. Ariz. 2016), https://cases.justia.com/federal/district-courts/arizona/azdce/2:2015cv01322/934023/45/0.pdf.

41. Brian Krebs, "Banks: Credit Card Breach at P. F. Chang's," *Krebs on Security* (blog), June 10, 2014, http://krebsonsecurity.com/2014/06/banks-credit-card-breach-at-p-f-changs.

42. P. F. Chang's China Bistro, Inc. v. Federal Insurance Co., No. CV-15-01322, 4 (D. Ariz. 2016), https://cases.justia.com/federal/district-courts/arizona/azdce/2:2015cv01322/934023/45/0.pdf.

P. F. Chang's paid the fees in order to maintain its ability to process credit cards and turned to Federal for reimbursement. Federal balked.

A federal judge analyzed the Cybersecurity by Chubb policy, which had an exclusion that stated: "With respect to all Insuring Clauses, [Federal] shall not be liable for any Loss on account of any Claim, or for any Expense . . . based upon, arising from or in consequence of any . . . liability assumed by any Insured under any contract or agreement."[43] The judge also analyzed the Master Services Agreement (MSA) between Chang's and its payment process, noting that "[i]n no less than three places in the MSA does Chang's agree to reimburse or compensate BAMS for any 'fees,' 'fines,' 'penalties,' or 'assessments' imposed on BAMS by the Associations, or, in other words, indemnify BAMS."[44]

Since the policy specifically excluded coverage for claims or losses due to contractual obligations, the court ruled that "the above referenced exclusions bar coverage for all three Assessments claimed by Chang's."

This is a very common exclusion, and since PCI-related fines are *not* assessed by regulatory bodies or a court of law, but instead are contractual obligations, organizations that seek coverage for credit card breaches should ensure that coverage for PCI-related fines and penalties are explicitly addressed.

Government-Sponsored Attack Exclusions

Another widespread exclusion that can have unexpected consequences involves "acts of war." It's standard practice to have some form of exclusion for claims or losses due to war—but these clauses can be quite broad and exclude any activity conducted on behalf of a government authority. Why is this a problem? Consider the following headlines:

- "Why the U.S. Was Sure North Korea Hacked Sony"—*CBS News* (2015)[45]
- "Google Reveals Gmail Hacking, Says Likely from China"—*Reuters* (2011)[46]
- "Russian Agents Were Behind Yahoo Hack, U.S. Says"—*New York Times* (2017)[47]

Many data breaches are perpetrated (or suspected to be perpetrated) by agents working for a government authority. For example, in February 2013, the forensics firm Mandiant published a famous research paper titled "APT1: Exposing One of China's Cyber Espionage Units." The researchers exposed a hacking group that they dubbed "APT1," and provided evidence to support the theory that the group was a government-sponsored unit of the People's Liberation Army (PLA). According to the report, "Our evidence indicates that APT1 has been stealing hundreds of terabytes of data from at least 141 organizations across a diverse set of

43. P. F. Chang's China Bistro, Inc. v. Federal Insurance Co.

44. P. F. Chang's China Bistro, Inc. v. Federal Insurance Co.

45. Bob Orr, "Why the U.S. Was Sure North Korea Hacked Sony," *CBS News*, January 19, 2015, https://www.cbsnews.com/news/why-the-u-s-government-was-sure-north-korea-hacked-sony.

46. Sui-Lee Wee and Alexei Oreskovic, "Google Reveals Gmail Hacking, Says Likely from China," *Reuters*, June 2, 2011, www.reuters.com/article/us-google-hacking-idUSTRE7506U320110602.

47. Vindu Goel and Eric Lichtblau, "Russian Agents Were Behind Yahoo Hack, U.S. Says," *New York Times*, March 15, 2017, https://www.nytimes.com/2017/03/15/technology/yahoo-hack-indictment.html (accessed January 20, 2018).

industries beginning as early as 2006. Remarkably, we have witnessed APT1 target dozens of organizations simultaneously. . . . We believe that the extensive activity we have directly observed represents only a small fraction of the cyber espionage that APT1 has committed."[48]

If your organization detects a data breach, should it matter whether the intruders are government-sponsored, members of organized crime groups, or solo operators? Data breach notification laws still apply regardless of the perpetrators' motives and affiliations. Yet if a forensic investigation turns up evidence that your breach originated from an APT1-related IP address, you might not be covered.

Here are some examples of "war" exclusions from different cyber policies, underwritten by Beazley, Ascent, and AIG, respectively. All three are broadly worded and exclude government-sponsored attacks, which would exclude many breaches:

- "[T]his Policy does not cover Loss or Damage directly or indirectly occasioned by, happening through or in consequence of war, invasion, acts of foreign enemies, hostilities (whether war be declared or not) . . . or requisition or destruction of or damage to property by or under the order of any government or public or local authority."—Beazley Breach Response specimen, War and Civil War Exclusion, 2016
- "We shall not be liable for any claim directly or indirectly arising out of or in any way attributable to: . . . Strikes or similar labor actions, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not) . . . or requisition or destruction of or damage to property by or under the order of any government or public or local authority." –Ascent U.S. v2.3, 2015
- "The Insurer shall not be liable to make any payment for Loss: . . . arising out of, based upon or attributable to any seizure, confiscation, nationalization, or destruction of a Computer System or Electronic Data by order of any governmental or public authority." - AIG CyberEdge Security Failure/Privacy Event Management Insurance, p. 4, 2013

Given the prevalence of state-sponsored hacking, it's wise to carefully review the wording of any "war" exclusions in your policy quotes. Consider requesting edits to narrow the scope, so that breaches that stem from government-sponsored actions are still covered.

Security Practices Exclusions

Cyber insurance, in some cases, provides clear, specific financial incentive for implementing cybersecurity best practices. "Insurance can provide a lever to speed up companies' adoption of standard risk management practices," wrote a report produced by the CRO Forum, "by taking into account companies' cyber hygiene practices in the underwriting process."[49]

However, general exclusions for "failure to maintain security standards" are typically so broad that they don't provide clear incentives and can be leveraged as an "out" for the insurer in

48. Mandiant, *ATP1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013) https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

49. CRO Forum, *Cyber Resilience: The Cyber Risk Challenge and the Role of Insurance* (Amsterdam, Netherlands: CRO Forum, December 2014), 8, https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-

the event of a major breach (as in the case of *Columbia v. Cottage Health*). "This is an extremely troubling exclusion as it adds an uncertainty to the coverage," writes Richard S. Betterley. "The problem is, what happens when the standards change, or there is a mistake, and the insured is out of compliance? For us, the exclusion is hard to accept and dangerous for the insured. An insurer may say that it would never apply the exclusion, but we would not be confident that it will never be applied in the future."[50]

In contrast, some policies specifically exclude coverage for claims that result from a lost or stolen device when it is *unencrypted*. In other words, if a laptop containing patient health information is stolen and the data was unencrypted, the resulting liability for data exposure would likely not be covered.

Exclusions of this type can dramatically reduce premium costs, but of course, they also leave the policyholder exposed to risk. The best approach is to ensure that portable devices are deployed with strong encryption and to implement an effective auditing program to prevent accidental lapses. For example, an analysis produced by Marsh for the Public Utility Risk Management Services said that the unencrypted device exclusion "can be removed with confirmation that the applicant stores data on portable devices in any encrypted format, or otherwise has procedures in place to prevent a loss of such data should a device be lost or stolen."[51]

In this way, insurers have become an important driver for implementation of cybersecurity best practices. For many organizations, there is no clear cost to insecurity. Boards and executives have a vague sense of risk, but there is no specific dollar figure associated with gaps in cybersecurity practices. Even when regulations protect sensitive data, such as patient health information or credit card numbers, fines and penalties are not consistently applied or calculated. As cyber insurance evolves, underwriters are becoming an important factor in developing cybersecurity best practices and providing incentive for adoption.

12.5.7 Research the Insurer

The value of your insurance policy depends on more than the words in the document itself. The quality of vendors on the insurer's panel impacts the level of service the policyholders receive in the event of a breach, which can directly impact the outcome. In addition, many insurers provide value-added services and resources for policyholders, which can help reduce cybersecurity risks.

12.5.7.1 Insurance Panels and Prior Consent

Make sure to review the providers listed on your insurer's panel of approved vendors. This can help ensure that you will be working with qualified, experienced service providers in the event of a breach.

As an example, in 2014, Sony Pictures Entertainment (SPE) negotiated new cyber insurance coverage (by expanding the broader Sony Corporation of America (SCA) coverage to include

50. Betterley, *Market Survey: 2017*.

51. Marsh, "PURMS: Summary of Cyber Coverage Policy Period: November 3, 2016," October 31, 2016, p. 3, http://www.purms.org/MeetingDocs/Board/Annual/2016/Marsh%20-%2010-31-16%20Cyber%20Proposal%20-%20Appendix%20D.pdf.

24-1.pdf.

SPE). The director of risk management for SPE reviewed the list of approved attorneys and emailed SCA to make sure that SPE's providers were approved prior to signing, as shown below:[52]

> From: Tetzlaff, Donna
> Sent: Wednesday, August 13, 2014 6:39 PM
>
> . . .
>
> Hi Kathy:
>
> On the schedule of firms for SCA there is listed Ropes & Gray LLC, that is one of our firms as well. We also see on the AIG's Panel Counsel List are Alston Bird and Baker Hostetler. We use these firms too.
>
> We would like to add:
>
> Baker Mackenzie [*sic*]
>
> Thank you.
>
> Donna

> From: Turck Rose, Kathryn
> Sent: Thursday, August 14, 2014 1:22 PM
>
> . . .
>
> Hi Donna,
>
> We have been informed that AIG confirmed they can add Baker McKenzie to the panel counsel list, subject to the rates of $500/$250/$100 already listed on the SCA policy.
>
> Regards,
>
> Kathy Turck Rose
> Director, Risk Management
> Sony Corporation of America

That's the way to do it—check in before you sign a policy or any time you have a change in your preferred vendor. Make sure to review not just the list of attorneys, but any provider you may wish to use—forensic investigators, PR firms, and the like. If you do need to add a provider, note that the insurer may set the rate, as AIG did with Sony. Rate caps are typically reasonable, but you should clear any rate limitations and payment terms with your preferred provider to ensure that there are no issues. When a breach occurs, you want to be able to get help as quickly as possible, so there are no unnecessary negotiations or conflicts in an already sensitive time.

---

52. "EM from K Turck-Rose to DT 8-13-14 AIG accepted Baker-Mackenzie.docx," WikiLeaks, accessed August 8, 2019, https://wikileaks.org/sony/docs/03_03/RISKMGMT/POLICIES/E%26O-Media-Tech-Cyber%20Liab/14-15%20Renewal/Cyber/Correspondence/SCA/EM%20from%20K%20Turck-Rose%20to%20DT%208-13-14%20AIG%20accepted%20Baker-Mackenzie.docx.

12.5.7.2 Value-Added Services

Today's cyber insurers offer much more than coverage. Many also provide valuable resources and services, from employee training videos to vulnerability scans, which are offered free or at a discount to policyholders. This is a win-win for the insurer and the policyholder: By making proactive training and security products more accessible, the insurer reduces risk and, presumably, saves money on insurance payouts.

As you review quotes and pricing, check out each provider's value-added services. Some of them can save you money, which may make up for differences in pricing. For example, many insurers offer policyholders access to a web portal with resources designed to reduce risk. These may include:

- **Security Awareness Training** - online training videos and quizzes to educate employees
- **News Center** - timely updates on cyber risk, security and compliance, upcoming events, and helpful links
- **Risk Management Tools** - useful tools for assessing and managing risk, such as online self-assessments, breach cost calculators, and policy templates
- **Learning Center** - whitepapers, articles, and recorded webinars

Other proactive free or discounted services can include:

- Vulnerability Scans
- Proactive Legal Advice
- Tabletop Exercises
- And more

12.5.8 Choose!

You've done all the hard work—now it's time to decide! Choosing your cyber insurance provider, of course, is typically an iterative process. You may wish to have one or two people take the lead and narrow down the list. Before you pull the trigger, make sure to loop in your key stakeholders again, to verify that you haven't missed anything important and to ensure that you have their buy-in. It's also important to get executive or board-level approval for any residual risk that will not be covered.

12.6 Leverage Your Cyber Insurance

Don't just buy cyber insurance and let your policy get dusty on a shelf. Your cyber insurance policy is one of the key elements of your cybersecurity and data breach response program. To get the most out of your investment in cyber insurance, you'll want to integrate your insurer's services into your policies and procedures, and build relationships with key members of their team.

Recall that to manage a data breach, your organization must have the following capabilities:

- **Develop** your data breach response function.
- **Realize** that a potential data breach exists by recognizing the signs and escalating, investigating, and scoping the problem.
- **Act** quickly, ethically, and empathetically to manage the crisis and perceptions.
- **Maintain** data breach response efforts throughout the chronic phase and potentially long-term.
- **Adapt** proactively and wisely in response to a potential data breach.

Let's discuss how your cyber insurance comes into play for each of these capabilities.

12.6.1 Develop

Once you sign a new cyber insurance policy, make sure to integrate it with your response function. Here are some key steps to take:

- Consider having a preliminary meeting with your insurer's breach response team, if available.
- Understand how and when to notify your insurer of a breach. Know what the insurer needs from you and what to expect in terms of response times and persons involved. Make sure that you carefully review any notification and documentation requirements, so you don't accidentally miss any notification deadlines!
- Note any contractual obligations required, such as documentation that you need to maintain with third-party providers, that you may need to provide to your insurer in the event of a breach. Make sure your legal counsel is aware of these requirements and has a plan for maintaining compliance.
- Develop a list of items that you will want to clearly agree upon in advance with your insurer, such as the names of approved providers for legal/breach response services, and any other items where advance approval would be appropriate. Ideally, you will already have your preferred vendors approved before you sign, but this list may change over time, and you need a process for keeping it up to date.
- Put together a list for your IT management that includes any technical requirements (for example, mobile device encryption) that you will need to have in place and documented for the insurance to be maximally effective.
- Review your insurer's cyber services and tools, and make a plan to take advantage of any training opportunities, policy templates, cybersecurity news alerts, or other resources.

12.6.2 Realize

When your first responders notice the signs and symptoms of a potential breach, you'll need to act quickly to notify both internal and external response teams. If your insurer also handles breach response services for you, then your team will need to reach out.

One tip for responders: In your internal communications, refer to a potential breach as an "incident" or an "event." Depending on state and federal laws, an event that might informally be referred to as a "breach" may not actually meet the legal definition. A common mistake that responders make early on is to refer to a "breach" in writing, even though actual data exposure has not been confirmed. In the event that you're subjected to regulatory investigations or lawsuits, the existence of email threads or documentation that refers to a "breach" can increase your liability.

The next step is investigation and scoping. Typically, you will work with a qualified attorney to manage the investigation and make the final call on whether notification is required. You may also need to engage the services of a digital forensics team to conduct evidence preservation and analysis. Your insurer may assign your service providers based on their panel, or you may be able to use your own provider, with prior approval.

12.6.3 Act

Take quick action to minimize reputational, financial, and operational damage. For example, actions may include working with a PR firm to issue a press release about a cybersecurity attack or outage. Your insurance may cover the costs of notification, call center services, credit monitoring, or other reparations.

12.6.4 Maintain

During the chronic phase of a data breach, coverage for legal fees and investigative response is particularly important. As you move into this phase, make a plan for managing potentially long-term expenses and human resources related to the breach. Will your insurer front the costs of ongoing legal fees, or will you need to plan for a reimbursement cycle? Will you be better positioned to leverage your insurance if you hire outside consultants, as opposed to leveraging in-house resources? Remember that lawsuits and investigations can last for years after a breach is announced. Make a plan early on for maintaining your response and working with your insurer long term.

12.6.5 Adapt

Review your coverage after a breach. What worked? What didn't? Do you need higher limits or a different type of coverage? Was your insurer easy to work with, or did you experience challenges?

12.7 Conclusion

Make sure to review and adjust your cyber insurance coverage at least annually and upon major changes to your environment or the threat landscape. New cyber threats emerge so quickly that a policy that was appropriate one year ago may need major changes to fit your current needs. Also, the cyber insurance landscape is changing very quickly, and new products may emerge that better suit your needs.

With cyber insurance, like technology itself, you shouldn't just "set it and forget it." Actively monitor your insurance and the state of the industry to ensure that you have the right coverage for today's risks.