I am particularly excited to present the Winter 2016 edition of Willis Towers Watson’s Cyber Claims Brief. This edition is the first of its kind from the insurance brokerage industry in that it centers on a set of data collected from the cyber claims we’ve reported to insurers during the last five years on behalf of our clients (“the Willis Towers Watson "Reported Claims Index"). We have incorporated within each article specific findings from the Reported Claims Index in order to provide additional, thought-provoking insight into some of the key trends of 2016, and what we expect to see develop in the coming year.

While much has previously been written in the privacy and security world about the dangers posed by hackers and the potential damages unauthorized network intrusions can cause, Emily Lowe and Berkeley Research Group’s Tom Brown take a closer look at the hackers themselves; specifically, who they are, what motivates them to carry out attacks and what they’re likely to do with the digital assets they’ve stolen.

Combining our Reported Claims Index with some of the results from a cyberrisk survey we commissioned this past summer to better understand organizations’ cyberrisk management priorities, Brian Weiss highlights the link between security awareness training for employees and the potential impact on frequency of employee-related cyberincidents.

As organizations continue to outsource various aspects of their businesses, the number of cyberincidents originating from third-party vendors continues to increase. Adeola Adele, in collaboration with Norton Rose Fulbright’s David Navetta and Matthew Spohn, discuss the increase in third-party-related breaches, answer some frequently asked questions regarding the respective responsibilities of the involved parties following a breach, and provide key considerations for drafting vendor contracts, as well as additional insured coverage under cyberinsurance policies.

As regulatory enforcement is ramping up, especially in the health care sector, Gina Macari hones in on some of the largest HIPAA settlements, claim trends and provides recommendations regarding insurance coverage for HIPAA fines and penalties.

Finally, recognizing that Network Business Interruption incidents are on the rise, Jim Devoe and Dan Twersky take on one of the most noteworthy cybercase studies of 2016, and opine on how a typical cyberinsurance policy might respond.

We hope you enjoy this edition and, as always, we look forward to your comments and feedback.

Kenneth Ross
Executive Vice President, Willis Americas Administration, Inc.
Director, FINEX Claims & Legal Group and Thought & Product Leadership
+1 212 915 8083
ken.ross@willistowerswatson.com

---

1 The Reported Claims Index is a collection of representative cyber claims of all different incidents, severity, and loss amounts we have selected for inclusion in our claims study mentioned throughout this edition of the Cyber Claims Brief, and to be incorporated into future editions.
Companies rely on technology and outsourcing for critical activities, including storing sensitive client data and intellectual property, communicating and conducting transactions. This leaves them vulnerable to cyberattacks. Whether from company insiders or outside hackers, these attacks can interrupt business operations, result in the theft of proprietary information, or cause the loss of customers’ data — with devastating effects on a company’s reputation and bottom line. The threat of litigation and increased regulatory scrutiny have broadened this risk and escalated potential losses.

The below charts created from the Willis Towers Watson Reported Claims Index highlight that organizations need to remain vigilant against threats to their network and information assets. While many organizations experience daily attacks on their networks, events causing significant damage appear to be uncommon. However, the results from our data suggests that when an attack does succeed, it impacts a disproportionately larger amount of personally identifiable information (PII), which has a greater overall financial impact than other claim categories. While hacking incidents accounted for only 17.28% of the incidents within the Reported Claims Index, they represented 71.9% of the total records compromised. Therefore, as organizations consider how best to protect themselves with technology, tools and procedures, those efforts may be less effective if organizations do not understand who is behind cyberattacks, how the attackers operate and what motivates them.
Hacktivism is the sprawling, loosely organized online group known as cyberattacks in support of an ideology. So-called “hacktivists” are cybercriminals who purport to commit crimes to advance their agenda, there are others who do. One such sub-group of criminal hacktivists was known as “LulzSec.” Its members used encrypted, invitation-only online chatrooms to plan attacks and an eponymous website and Twitter account to spread propaganda, seek monetary support in the form of Bitcoin donations, taunt victims and dump stolen information online. United States federal prosecutors charged the core leadership of LulzSec, which comprised individuals living in the United States, the United Kingdom and Ireland and who ranged in age from their late teens to mid-twenties, with a variety of hacking offenses. LulzSec’s leaders and their co-conspirators broke into computer systems used by several media companies and government entities, among hundreds of other victims in the education, financial services, travel and entertainment, technology, media, health care and consumer products sectors. These hacks resulted in the theft and disclosure of PII of over one million victims, not to mention the remediation costs suffered by the organizations whose computer networks were compromised.

### Nation state actors
Nation state actors can be classed as foreign government agents or cybercriminals working on their behalf and whose agenda can range from stealing economic information to launching disruptive or destructive attacks. In the case of the *United States v. Wang Dong,* et al., federal authorities charged five members of the Chinese military with hacking into computer systems owned by six American victims in the U.S. nuclear power, metals and solar products industries with the purpose of stealing information useful to competitors in China, including state-owned enterprises. In the *United States v. Amad Fathi* et al., seven hackers who were sponsored by the Iranian government were charged with disabling the websites of 46 major companies in the United States, primarily in the financial sector, which cost the victim organizations tens of millions of dollars in remediation costs.

### Rogue employees
Malicious insiders, often disgruntled employees, seek to take advantage of their privileged access to steal valuable information or disrupt or destroy computer systems. A scheme involving a trader at a large bank illustrates this type of attacker. Recruited by a competitor to build a high-frequency securities trading platform, the employee, who was unable to do the work on his own, stole the necessary computer code worth millions of dollars from his employer. Indeed, rather than use any sophisticated means of attack, the employee took advantage of his insider status simply to print out the computer code on hundreds of sheets of paper, which he took home and analyzed. Charged with economic espionage, the employee was found guilty in federal court following a two-week trial.
How do hackers infiltrate victim computer networks?
The means by which outside attackers gain unauthorized access to computer systems varies widely, from the low-tech to the most sophisticated manipulations. Simple attacks, like phishing emails which carry a malware payload, are often surprisingly effective and can permit a hacker deep access to a target network. On the other end of the scale are hacks which rely on the exploitation of known, but unpatched vulnerabilities in computer systems, or even so-called “zero days,” undetected flaws that are known only to the attacker. A basic rule of thumb is that no matter the means, a determined hacker will eventually be successful. Time is on the attacker’s side, whereas a computer network administrator needs to prevent attacks 100% of the time.

How can clients lower the likelihood of a hack?
There is no one-size-fits-all approach to cybersecurity — every organization is different. There are, however, some basic elements that companies may wish to consider as a means of reducing their cyberrisk. A starting point is the development and implementation of a comprehensive information security plan. Once applied, such a plan should be reviewed and updated regularly in light of the often dynamic nature of computer networks and the threat environment. A comprehensive information security plan may include, among other things, a cyberrisk assessment, involving external penetration testing (sometimes called ethical hacking, in which external cyberdefenses are tested), as well as an internal evaluation. For example, are software patches applied in a timely fashion? Is the network adequately segmented? Are network logs appropriately detailed and maintained?

The two questions above are commonly asked by insurers on applications for cyberinsurance. The latter question may be especially relevant to investigating a hack. Logs may provide valuable forensic data, potentially permitting an investigator to look back and determine how a hack occurred, whether a system is still compromised, and what data, if any, was exfiltrated. In addition, a comprehensive information security plan may also include an incident response blueprint. Speed is often important in dealing with a cyberattack, and a “break glass” incidence response plan may increase the efficiency of a response and help with the preservation of data important to a forensic assessment. Finally, organizations may wish to consider their culture of security. Engagement by senior management coupled with regular training, which raises awareness among employees, may help defend against low-tech attacks like phishing emails and promote an overall emphasis on cyberdefense.

Taking these steps will help prevent or reduce the frequency of hacking claims and the associated financial loss and reputation damage.
The reliance on third-party vendors, whether directly or indirectly, has increased dramatically with technological advancements and competition. At the same time, several studies have reported that loss or compromise of data in the hands of such third-party vendors accounts for a significant percentage of all data breaches or cyberattacks. For example, according to the Ponemon Institute report of May 2016, 75% of the IT and security professionals surveyed stated that the risk of a third party’s breach is a serious concern and increasing within their organizations. This view appears to be supported by Willis Towers Watson’s data which indicates that of the Reported Claims Index, data held by third parties accounted for 27% of the total 112,890,290 lost or otherwise compromised records involved in those claims.

As shown on the above chart, third-party cyberincidents were more prevalent in the retail, financial services and health care industries.

Notably, the cost on the black market of stolen financial and health care records — records likely to be controlled by a vendor — is far greater than that of other stolen records given the value of such information, including their use in social engineering schemes and other criminal acts. One recent study found that a breach involving medical records, customer financial records or credit cards will cost a company an average of $7 million in 2016, when lost customers are factored. Analyzed in another way, the cost averaged $221 for each lost or stolen record. (See https://securityintelligence.com/media/2016-cost-data-breach-study/). Given the potential costs associated with loss/disclosure of customer data, below are some of the questions that companies ask when negotiating vendor contracts:

If my vendor is breached that’s the vendor’s problem, right?

Unless a contract states otherwise, it is almost always true that an organization has ultimate responsibility for breach of its data while in the hands of a vendor. According to data breach statutes enacted in the majority of states, the owner of the personal data — not the vendor who is handling it — has the primary obligation to investigate the breach and provide any required notice to the affected individuals. The same is true with respect to medical information protected by federal and state laws.

Accordingly, if the organization’s sensitive data is breached while under the control of a vendor, the vendor’s primary obligation is to notify the organization. It is then the customer’s obligation to handle the fallout, unless the customer’s contract with the vendor provides otherwise.

My vendor warrants that it will keep my information confidential, won’t that protect me?

Even where the vendor unequivocally warrants that it will keep the customer’s data confidential, there is the question of the remedy for breach of that warranty. The typical vendor contract contains a section titled “limitation of liability” with two key provisions: one capping the vendor’s total liability (often the total fees paid under the contract, or fees paid in the prior 12 months), and another stating that in no event will the vendor be liable for any consequential, incidental, or indirect damages (typically known as a “consequential damages waiver”).

The damages cap is straightforward: even for a breach of the contract, the customer cannot recover more than that cap from the vendor. Careful consideration should be given to whether that cap adequately protects the company in the event of a data breach.

But organizations must also pay close attention to the consequential damages waiver. The law generally defines consequential damages as those damages that are not foreseeable to a stranger to the contract, but are foreseeable to the parties to a contract at the time they signed it, given what they know of the transaction. But even judges will admit that this definition is difficult to apply in practice. The result is that in the case of a data breach, one could argue that some or all of the resulting damages — costs to notify affected individuals, costs to respond to regulators’ investigations, etc. — are
consequential damages. If that is correct, then a consequential damage waiver will bar any recovery of those damages. As a result, customers need to pay particular attention to any consequential damages waiver in a vendor contract.

My vendor contract has an indemnity clause, won’t that protect me?

In addition to warranties and damages limitations, most vendor contracts will contain some sort of indemnity provision. For instance, a basic indemnity provision would require the vendor to “defend and indemnify Customer against any third-party claim, suit, or proceeding arising out of Vendor’s material breach of this Agreement.” Such indemnity clauses are often carved out from the contract’s damages cap and consequential damages waiver. However, standing alone, they may not provide adequate protection against data breaches.

The primary limitation of a standard indemnity clause is that it may only cover lawsuits brought against the customer as a result of the data breach (assuming the contract is drafted so that the data breach qualifies as a breach of the agreement). Such third-party claims, though, are a relatively rare consequence of a data breach. Where millions of customer records are breached, one can expect a class action lawsuit brought on behalf of the affected individuals. Data breaches with less than 100,000 affected individuals are less likely to interest a plaintiff’s lawyer, who typically is only paid a percentage of the final recovery.

In such cases, the more likely consequences are the costs to comply with the relevant data breach notification statutes and to address the public relations issues. These include the costs of hiring forensic investigators to assess and remediate the breach; attorneys’ fees to determine the legal obligations triggered by the breach, and to respond to any investigation by state regulators or law enforcement; costs of identifying affected individuals and sending the required notices; costs to set up and staff call centers; costs of credit monitoring services that may be offered to affected individuals; and potential regulatory fines and penalties imposed by state agencies. An indemnity clause can be drafted to shift responsibility for all these costs to the vendor in the event of a data breach, but such language is unlikely to be found in the vendor’s standard contract.

Will a well-drafted vendor contract fully protect me?

The best contract is only so good as the other side’s willingness or ability to perform. Where there is a claim for breach or indemnity, the other side may be motivated to fight the claim in litigation. Such litigation can be expensive and time-consuming. Even if the vendor contract provides that the loser pays the winner’s attorneys’ fees, recovery can be delayed by the litigation and appeals process. At the end of that litigation (or even if there is no litigation at all), there is always the question of collectability — does the vendor have sufficient assets to satisfy a judgment? If not, then the organization’s contractual protections could be rendered virtually worthless.

What if I have the vendor add me as a named insured on its cyberinsurance policy?

Cyberinsurance policies are intended, among other coverages, to protect loss or disclosure of the insured’s data, and they can provide additional protection against third-party data breaches. When the insured vendor has agreed to indemnify its customer for loss or disclosure of the customer’s data, the vendor may want to amend its insurance policy to include the customer as an “additional insured.” The customer may want this as well, as it can help protect against any claims brought against the customer due to the vendor’s wrongful acts or errors.

However, the scope of coverage would depend on the type of services the vendor has agreed to provide to its customer. For example, where the vendor’s services include direct access to the customer’s network or when the vendor holds the customer’s confidential data, the vendor’s technology errors and omissions policy should include network security and privacy coverage. In this case, the coverage can be written to include loss, disclosure and theft of data in any form, as well as network security failure, denial of service attacks, and transmission of malicious code. If agreed by contract, the coverage can also be negotiated to include some first-party costs such as: data breach regulatory fines and penalties, the cost of notifying individuals of a security or data breach, the cost of credit monitoring services and any other related crisis management expense.

If a customer is named as an additional insured, then to allow coverage for a claim brought by the customer against the vendor, the policy’s Insured v. Insured exclusion may also need to be amended. If it is not, the insurer could invoke it to avoid covering any obligation that the vendor may have to its customer. Similarly, the contractual liability exclusion — which typically precludes coverage for any liability the insured assumed under a contract — may need to be deleted or amended to provide an exception for the vendor’s contractual indemnification of its customer. This amendment, however, is more difficult to achieve as most insurers consider the insureds’ contractual obligation to be pre-existing and not necessarily one that flows from the cyberincident. As such, after reviewing the vendor contract, insurers will typically only provide a carveback for certain losses (such as Payment Card Industry fines and penalties) rather than all damages contemplated under the vendor contract.

Additional issues are raised if the customer also purchases cyberinsurance and the vendor has agreed to provide “additional insured” coverage. In that case, the customer should consider
amending the “other insurance” clause of its own cyberinsurance policy to ensure that the vendor’s policy would apply as primary insurance in the case of a breach caused directly or indirectly by the vendor. It is worth noting that unless the policy is otherwise endorsed, the vendor and its insurer may then have full control of the claim, including selection of breach counsel, forensic investigators, public relations and any other first-party loss protection offered under the policy.

Ultimately, the goal of the “additional insured” coverage afforded to the customer is to ensure that coverage is being provided only for claims arising from the vendor’s wrongful acts or errors, whether directly or indirectly (rather than the acts or errors not within the vendor’s control). Providing insurance coverage to the customer beyond that which is contractually or legally required could unintentionally limit the coverage available to the vendor for its own wrongful acts.

**Conclusion**

There is no “one size fits all” protection against the risks presented when vendors have access to customers’ data. Those risks are best addressed in consultation with attorneys, insurance advisors and brokers, and any in-house security or IT personnel. Some of the topics to be discussed with those advisors include:

- What are the risks inherent in the types of data that the vendor will have access to? Does it include Social Security numbers, medical information, credit card information or other data subject to state data breach laws? Does it include other information that is not subject to those laws, but could cause harm or embarrassment if disclosed?
- Is there a way to limit the data to which the vendor has access? If not, can it be encrypted to lessen the risks of breach, or can other prophylactic security measures be employed?
- What are the potential costs and consequences in the event the company’s data is breached in the hands of the vendor, and how can the vendor’s contract properly allocate those risks? If the vendor refuses to accept the proposed terms, are there other ways that the risks can be addressed? If not, does the company need to look at other vendors?
- Consider working with an attorney to create your own template for your company’s vendor contracts, with robust terms addressing the company’s rights and remedies in the event of a data breach. Many vendors will agree to at least start with the customer’s template when negotiating an agreement. However, counsel should still be consulted when vendors attempt to negotiate changes to the agreement, and especially those provisions addressing confidentiality, warranty, indemnification and limitation of liability.
- Prevention is the best medicine: due diligence on a vendor’s data security protocols may help identify vendors who present a higher risk of a breach, and investigation into a vendor’s finances may help determine whether the vendor can satisfy its obligations in the event of a breach.
- The role of insurance: when carefully crafted, insurance can help mitigate the costs associated with loss of customer data but, to the extent possible, it must be aligned with the obligations assumed or transferred under the vendor contract.

---

Willis Towers Watson has arranged for Norton Rose Fulbright US LLP to offer its clients a unique service starting in January 2017. For a special flat fee per contract, Norton Rose Fulbright will analyze companies’ contracts with their vendors and rate the contracts terms addressing cybersecurity and privacy risks. Clients will receive a report explaining contract’s strengths and weaknesses, and identifying areas of risk. Contact Jason Krauss, Cyber & E&O Product Leader at 212-915-8374 or jason.krauss@willistowerswatson.com for more information.
The human element of cyberrisk
Why it pays to sweat the small stuff

By Brian Weiss

This summer Willis Towers Watson commissioned a survey of 306 risk, finance, human resources, information technology and operations decision makers to gain insight into their organizations’ cyberrisk priorities. Of those surveyed, 64% indicated that human capital and employee solutions are a very important focus for cyberloss control, and 36% indicated they are a somewhat important focus. Looking at a longer horizon, 68% viewed human capital and employee solutions (which includes cybersecurity awareness training) as a very important future focus for their organizations.

Interestingly, those we surveyed with roles in information technology and operations were more focused on employee solutions than the other interview groups. Both groups had over 70% of participants viewing employee-related cyberrisk as very important. Conversely, of those surveyed in risk and finance, only 55% deemed human capital and employee solutions as a current very important focus. The results highlight the need for organizations to focus more attention and resources to cyberrisk created by employees and their role in overall cyberrisk mitigation.

In the Summer 2016 edition of the Cyber Claims Brief we noted that employees are the first line of defense for companies. We described the risk created by employees and how IOT (the internet of things), BYOD (bring your own device) policies, and the changing face of the workforce combined to accelerate that risk. The Willis Towers Watson Reported Claims Index provides additional support for this reality — the number of cyberincidents involving lost data by the negligence of employees far exceeds the number of incidents caused by bad actors.

### Percentage of Claims By Breach Type

<table>
<thead>
<tr>
<th>Breach Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accidental Disclosure</td>
<td>32.72%</td>
</tr>
<tr>
<td>Lost/Stolen Devices</td>
<td>21.43%</td>
</tr>
<tr>
<td>Hack</td>
<td>17.28%</td>
</tr>
<tr>
<td>Rogue Employee</td>
<td>11.52%</td>
</tr>
<tr>
<td>Third-party Breach</td>
<td>7.6%</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>3%</td>
</tr>
<tr>
<td>Network Business Interruption</td>
<td>2.07%</td>
</tr>
<tr>
<td>Other</td>
<td>7.13%</td>
</tr>
</tbody>
</table>

Approximately one-third (32.7%) of all cyberincidents in the Willis Towers Watson Reported Claims Index are caused by accidental disclosures, with lost (or stolen) devices accounting for another 21% of incidents. This trend was most pronounced in the health care industry, where almost half of our clients’ cyberincidents can be attributed to accidental disclosures, and another one-quarter due to lost/stolen devices. Clients in the education sector also had a pronounced trend of cyberincidents stemming from employee accidental disclosures or lost devices, with approximately two-thirds of their incidents falling into these categories.
Claims included within the employee error or negligence category are those involving lost laptops or mobile devices, negligent disposal of paper records with PII in an unsecured manner, or personal files accidentally sent by email to an unintended recipient. Accordingly, it’s important that organizations, especially those in the health care and education sectors, take special note of the risk caused by employee accidents and implement training and loss control measures focused on employee behavior.

While accidental disclosures and lost devices together combine for the highest percentage of cyberincidents, the silver lining to this data is that the records lost in these claims represent less than 1% of the total records lost. To compare, hacks and third-party breaches account for approximately 90% of the total number of records lost. But that does not allay the concerns regarding employee conduct, as employees are most likely to be the source of the next cyberincident, and each incident can be costly.

Even though accidental disclosures and lost device cyberincidents generally do not result in high record loss cyber claims, the large quantity of claims may nevertheless prove costly — whether for a breach coach, legal costs, forensics or public relations — which may be less than the applicable self-insured retention (SIR) on a cyberinsurance policy. Depending on the insurer, the retention may apply to the number of individuals notified, the cost of the overall incident response, or both. This means an organization will have out-of-pocket costs for each of these events. That is not to mention the lost productivity cost associated with mitigating or remedying the breach.

For companies at a higher risk of multiple, low severity employee-based incidents, it may be advantageous to procure a cyberinsurance policy that provides consultative assistance from a breach coach (usually the most costly component of a low severity breach response) with no SIR.

In conclusion, the most common cyberincident that a company faces will be rooted in employee conduct, as borne out by the Willis Towers Watson Reported Claims Index. It is therefore crucial that organizations focus on cyberrisk posed by its employees, and develop appropriate risk mitigation strategies, including encouraging regular security-conscious behavior and implementing continuing and regular awareness training.
Industry spotlight
Health care

By Gina Macari

The success of a business is increasingly defined by the strength of its technology, making data privacy and security a necessity and top priority for business survival. This is true for industries such as retail, education and hospitality, but no sector has felt the burden of the responsibility to protect private data more than the health care industry. Companies in the health care industry routinely maintain thousands of patient records containing the full spectrum of personally identifiable information and personal health information (PII and PHI) such as Social Security numbers, addresses, insurance policy numbers, medical diagnosis details and even credit card information. These organizations face vast exposure to privacy violation claims when systems are hacked, devices are stolen, or privacy procedures are thwarted — and even when employees make innocent mistakes.

The Willis Towers Watson Reported Claims Index reveals that the vast majority (81%) of claims made against health care organizations result from three breach types: (1) accidental disclosure of data (42%); (2) loss or theft of devices such as laptops and phones (26%); and (3) theft or misuse by rogue employees (13%). While hacks comprise only 6% of total breaches included in the Willis Towers Watson Reported Claims Index, hacks account for the highest number of records lost per breach. In fact, as shown in the chart on page 12, hacks represent the majority of the lost records containing PII and PHI. These observations are consistent with and supported by various other studies, such as IBM’s 2016 Cyber Security Intelligence Index. In that study, which was based on data collected from between January 1, 2015 and December 13, 2015, IBM noted that more than 100 million health care records were compromised, and from more than 8,000 client devices in over 100 countries.

With every lost record comes the possibility of exposure to a wide variety of claims and resulting costs. Aside from the potential reputational damage and loss of customer confidence, those organizations that have been victims of hackers have a profound understanding of the scope of financial liability that can result from being hacked. According to the “Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data”, a study commissioned by ID Experts, Ponemon Institute estimated that data breaches may cost the healthcare industry $6.2 billion in 2016.

One of those costs includes the fines and penalties levied by the U.S. Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPAA). In this regard, HHS’s data reflects that HIPAA settlements are on the rise, largely due to the agency’s aggressive enforcement proceedings against health care organizations. In the first 10 months of 2016 alone, the health care industry paid out just short of $21 million to settle HIPAA violations.

Top 10 HIPAA settlements (2014-2016)

<table>
<thead>
<tr>
<th>Settlement (in millions)</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5</td>
<td>August 2016</td>
</tr>
<tr>
<td>4.8</td>
<td>May 2014</td>
</tr>
<tr>
<td>3.9</td>
<td>March 2016</td>
</tr>
<tr>
<td>3.5</td>
<td>November 2015</td>
</tr>
<tr>
<td>2.75</td>
<td>July 2016</td>
</tr>
<tr>
<td>2.7</td>
<td>July 2016</td>
</tr>
<tr>
<td>2.2</td>
<td>April 2016</td>
</tr>
<tr>
<td>2.14</td>
<td>October 2016</td>
</tr>
<tr>
<td>1.725</td>
<td>April 2014</td>
</tr>
<tr>
<td>1.55</td>
<td>March 2016</td>
</tr>
</tbody>
</table>

The $5.5 million settlement in the above table involved an incident which began with the theft of laptops during a burglary at one of the company’s facilities. Later, another laptop was stolen from an unlocked car. The investigation by HHS’ investigative arm, the Office of Civil Rights (OCR), revealed that 2,000 patient records were potentially compromised, including the PHI of four million individuals. The $5.5 million settlement reflects the government’s goal to send a strong message to entities covered by HIPAA: that failure to comprehend the risk presented by stored PHI and take appropriate steps to protect it will not be excused.

As a result of the increasing exposure to HIPAA fines and penalties, those in the business of managing risk in the health care space may find themselves searching for more answers to an old question:
How does cyberinsurance respond to HIPAA fines and penalties?

Many cyberinsurance policies expressly provide coverage for fines and penalties imposed by regulatory agencies, such as HHS, for violations of privacy laws.

A still lingering question, however, is whether HIPAA fines and penalties constitute uninsurable punitive damages. The answer to this question is unfortunately unclear and depends on a number of considerations, including whether: (1) the penalties are assessed for willful or intentional conduct; (2) the penalty is “punitive” rather than “compensatory;” and (3) the penalty is assessed directly against an Insured rather than vicariously.

To date, insurers have confirmed, through claim payments, that their intention is to cover HIPAA fines and penalties. While some cyberinsurance policies may include most favorable jurisdiction provision with respect to punitive damages, they are often silent regarding whether the same provision applies to HIPAA fines and penalties. As such, it is imperative that health care organizations work closely with their brokers to negotiate the most competitive wording available. Additionally, to the extent a court or insurance authority in a particular state could determine that portions of fines and penalties awards/assessments are uninsurable as a matter of public policy (based on any of the considerations above), organizations may also wish to consider obtaining fines and penalties wrap coverage offered through Bermuda markets. Because Bermuda markets are not subject to the same limitations regarding insurability of certain damages (e.g., choice of law under Bermuda policies tend to apply the Law of England and Whales, which is favorable to insurability of punitive damages) that are deemed punitive, the fines and penalties wrap policy coverage would “wrap-around” the primary domestic cyberinsurance policy and would fill any coverage gap in the event of a challenge on the grounds of insurability.

Finally, it is recommended that cyberinsurance policies contain coverage not only for the fines and penalties levied, but also for costs incurred in connection with the regulatory investigation of the alleged privacy violation, as these sums can be substantial.

---

4 https://www.hhs.gov/ocr/newsroom/index.html
5 see footnote 4
The day the internet went missing

By Jim Devoe and Dan Twersky

A growing category of cyberincidents is Network Business Interruptions. While representing only 2.07% of incidents within the Willis Towers Watson Reported Claims Index, we see this category as increasingly significant. Not only do such claims have the possibility to result in catastrophic first- and third-party losses, but recent attacks have achieved far greater ingenuity and sophistication, creating new ways and tools for attackers to perpetrate such schemes.

The Dyn attack

A distributed denial of service (DDoS) attack against Dynamic Network Service, Inc. (Dyn), a major Domain Name Server host, created a wide ripple of disruption across the internet. DNS providers help ensure that an internet user ends up at the correct destination after entering a web address into their browser. The attack flooded Dyn’s servers with so much traffic — reportedly 1 Terabit per second (akin to downloading the Library of Congress every two minutes) — that business customers who rely on Dyn to connect users to their sites, including major online social media, e-commerce, streaming video and audio, and content hosting companies, were disrupted to varying degrees. The sites were actually up and running, but merely appeared to be down.

Not only were the effects of this attack notable, so too was the source of the attack. Reportedly hundreds of thousands (if not tens of millions) of baby monitors, DVRs, security cameras and similar devices — collectively making up the internet of things (IoT) — were orchestrated to launch the simultaneous attack. Dyn advised the next day that the attack on their services came in three waves, none lasting more than two hours.

Business customers of Dyn reported similar disruptions as a consequence. A major cloud services provider advised that its service was affected during the first wave, for a similar timeframe. Others had differing impacts as the attack spread from the East Coast to West Coast and Europe. Customers of these businesses, in turn, felt the impact, whether it was the inconvenience of a streaming video being disrupted, or a business disruption arising from the inability to access the cloud provider’s servers.

Finally, the manufacturer of the underlying technology common to many if not all of the devices leveraged in this attack, was forced to recall millions of their devices for upgrades.

How might cyberinsurance respond to an attack like this?

Network interruption

Known also as business interruption, this coverage provides an insured with coverage for lost earnings and extra expenses incurred due to an interruption of its own system. This coverage requires the insured to clear a waiting period — a minimum amount of time that must elapse before any interruption is covered. A typical waiting period is eight hours, but can vary depending on the type of business being insured.

Dependent network interruption

Similar to network interruption, this coverage provides insureds with protection when they suffer losses arising from a third-party system interruption. Using these events to illustrate, the insured here would be one of Dyn’s customers, who themselves suffered a loss of earnings and/or incurred extra expense due to Dyn’s systems being interrupted by the attack. The waiting period would be similar here, and other limitations may apply such as co-insurance or sublimits.

Breach response

For the insured which is directly attacked, breach response may provide some coverage for costs incurred. This coverage is usually thought of in the context of a privacy breach, and is generally tailored to related expenses such as the legal determination of privacy obligations state by state, notification of affected consumers, and the offering of credit/identity monitoring protection and fraud resolution services. While the attacks in this case were not privacy related, they nonetheless could trigger some additional aspects of breach response coverage including the costs of cyber forensics to “put out the fire,” and the public relations costs intended to mitigate potential damage to the insured’s brand and reputation.

Percentage of claims by breach type

- Employee negligence or malfeasance: 3%
- External threat actor: 2.07%
- Social engineering: 2.30%
- Network business interruption: 17.5%
- Cyber extortion: 9.1%
- Other: 66%
Liability

Last but not least is liability coverage. Cyberinsurance policies will typically include liability coverage for claims alleging an insured’s negligence in protecting systems and information. These claims can be from any affected party who can allege some level of damage, and can range from a single affected party (Dyn’s direct customer, for instance) to a broad class action by downstream customers for the disruption of services for which they paid consideration. A second type of liability could arise if Dyn’s commercial customers allege negligence in rendering agreed to professional services, violating contractually agreed upon and paid-for service levels.

Considerations and takeaways

Awareness

The emergence of the IoT leads to new variants of old threats. The notion that baby monitors could be unexpected participants in a massive DDoS attack such as this is alarming, and awareness that this is possible is important. As we understand how the IoT actually works — that these intelligent devices are basically miniature “PCs” with less control and visibility to their owners — it’s not difficult to see how these devices could be hacked and misused. This recognition is a first step toward better preparing for this emerging threat.

Preparedness

Risk detection and mitigation steps by sophisticated tech companies limited the duration of loss suffered by these firms. The aforementioned cloud services provider, for instance, was able to re-direct to other service providers and minimize their reliance on Dyn during the attack, and the effective duration to them (and to their customers in turn). Clients should be asking themselves whether they are fully prepared for a similar threat; specifically whether the necessary risk detection and mitigation safeguards are in place.

Risk transfer

Cyberinsurance can provide a valuable and flexible tool for addressing many types of cyberlosses, and the attacks on Dyn are no exception. In fact, they underscore the need for Business Network Interruption coverage despite the historical low frequency of these types of attacks. Ensuring that Business Interruption coverage is in place in advance of a loss, that it includes the broadest possible terms and conditions, keeps up with rapid developments in these evolving areas of coverage, and is acted upon at the time of loss through proactive claims advocacy, are critical ingredients to successful risk transfer.
About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW ) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 39,000 employees in more than 120 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.