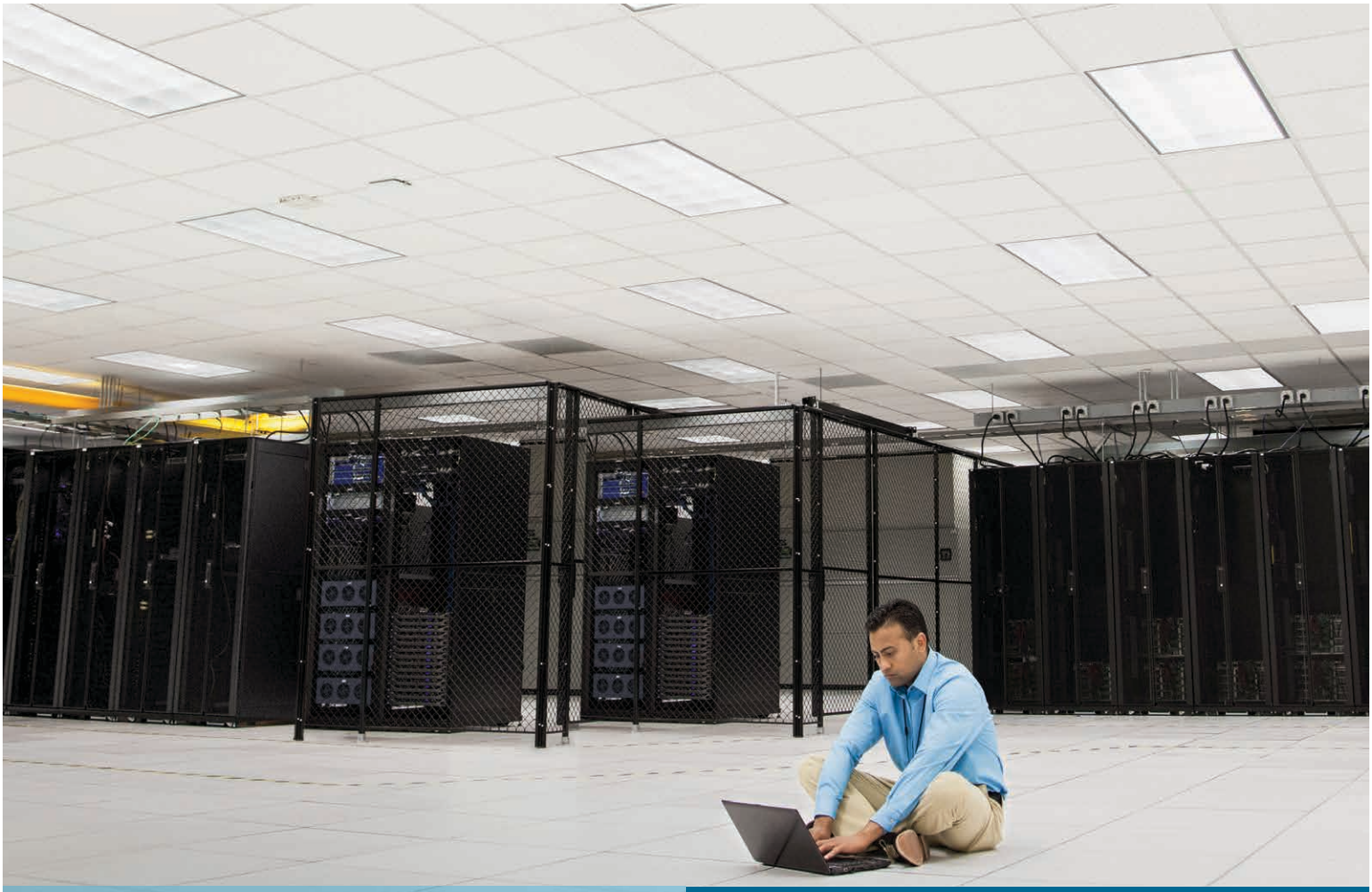

INTO THE BREACH

An intro to Starr Companies' Cyber liability practice

Accident & Health | Aviation & Aerospace | Casualty | Construction | Crisis Management | **CYBER**
Energy | Environmental | Financial Lines | Marine | Professional Liability | Property | Public Entity
Specialty Products | Travel Assistance

STARR COMPANIES
GLOBAL INSURANCE & INVESTMENTS

TRUTH IS STRANGER THAN FICTION

How Sony's mammoth data breach defines cyber risk

Photo courtesy Sony Pictures

When Sony refused to pull its action-comedy, The Interview, which lampooned North Korean Kim Jong-un, the company suddenly found itself under a crippling cyber attack.

Sony Pictures Entertainment cyberattacked

2014 was an unkind year to Sony Pictures Entertainment. The movie studio had struggled to produce blockbusters all year long, and as it headed toward Thanksgiving, it was on track to deliver earnings more than 11% down from the previous year and an operating loss of some $239 million. What the studio needed was a hit, and fast. Thankfully, studio executives thought, it had one: an action-comedy holiday release called *The Interview*, in which two bumbling television talk show personalities are recruited by the CIA to assassinate North Korean dictator Kim Jong-un.

What Sony didn't expect was that on November 24, a hacker group calling itself the Guardians of Peace would begin a protracted cyberattack upon SPE that entailed at least eight different dumps of sensitive company information to the public. This included leaking unreleased movies, confidential financial data (including executive salaries) and reams of internal correspondence that showed Sony's internal management to be dysfunctional, adrift and leaderless. The hackers also took over company websites and social media accounts.

The worst came on December 8, when the Guardians of Peace, which had roundly criticized Sony for the premise of *The Interview* during its previous attacks, made threats against actual theaters planning to show the movie. Sony pulled *The Interview* from release and temporarily halted all production work as it scrambled to protect itself. North Korea's largest cyberwarfare division, Unit 121, was widely suspected of orchestrating the attack, but the true culprits have never been fully identified.

Sony publicly stated it would set aside $15 million to cover losses from the cyberattack, but industry watchers suspect the true losses of the event, taking into account lost productivity, might reach $100 million. And while that is less than the $171 million in damages caused by a 2011 hack against the Sony PlayStation Network, it still is a major data breach that speaks to the severity of cyber risk in general.

...Sony was by no means the largest or even the most costly data breach of 2014 .

And yet, for as much media attention, financial damage and operational havoc as the Sony cyberattack caused, it was by no means the largest or even the most costly data breach of 2014. And that is the real story that the Sony event underscores: the risks of cyber liability—data breaches, denial of service attacks, theft of sensitive information and other hazards—are developing and expanding at such a rapid and unpredictable pace as to make all previous efforts to contain them of questionable efficiency. In short, this is the golden age of the hacker, and everyone—from private citizens and charitable organizations to businesses and governmental offices—is at risk.

But there is a solution—cyber insurance. While various carriers offer coverage against different kinds of cyber attack, Starr offers a comprehensive, carefully tailored product that syncs well with other insurance coverages. This makes not only for a compelling cross-selling opportunity within Starr, but it is also a much-needed solution for a business world under siege by digital troublemakers, ranging from thrill-seeking hooligans to sophisticated international cybercrime rings.

WHAT IS CYBER RISK?

An overview of the new threat to everything

Cyberattacks and data breaches get a lot of media attention, both because the hazards they represent are ever changing and sometimes difficult to comprehend. It has not helped that there have been some extremely large and high-profile cyber events in recent history—including one data breach at a prominent health insurer in early 2015 that involved some 80 million records of personal health information.

But what is the level of risk, really? Perhaps the best place to look is the Privacy Rights Clearinghouse, a consumer education and advocacy nonprofit that maintains a detailed database of data breaches going back to 2005. It breaks down data breaches into seven basic categories:

Unintended disclosures. Sensitive information posted publicly on a website, mishandled or sent to the wrong party by e-mail, fax or mail.

Hacking or malware. Unauthorized electronic entry by an outside party, malware or spyware.

Payment card fraud. Fraud involving debit and credit cards that is not accomplished via hacking, such as skimming devices at point-of-service terminals.

Insider. Someone with legitimate access—such as an employee or a contractor—intentionally breaches information.

Physical loss. Lost, discarded or stolen nonelectronic records, such as paper documents

Portable devices. Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.

Stationary devices. Lost, discarded or stolen electronic devices not designed for mobility, such as desktop computers or racked servers.

Unknown or other. Typical of cases where the actual cause of loss is never identified.

For 2014 alone, the Privacy Rights Clearinghouse had 294 data breaches on file, each ranging from a handful of compromised records to many millions of them. Of these, hacking was by far the most common cause of loss:

Data Breaches —causes of loss

TYPE OF BREACH	# OF OCCURRENCES (% OF TOTAL)
Hacking	146 (49.6%)
Unintended disclosure	49 (16.6%)
Portable devices	39 (13.2%)
Insider	26 (8.8%)
Physical loss	16 (5.4%)
Stationary devices	8 (2.7%)
Unknown	8 (2.7%)
Payment card fraud	2 (0.6%)

This represents an important shift in loss history, as previous industry White papers and reports had pointed out insiders and unintended disclosures as the biggest threats to data security. As 2014 showed, however, digital intruders are now the biggest concern.

But what kinds of operations are hit most often? According to the Privacy Rights Clearinghouse, there are seven basic categories: financial and insurance services businesses; retail businesses; other businesses, educational institutions; government and military; healthcare and medical providers; and nonprofit organizations.

Of these, healthcare and medical providers were the most frequent target in 2014, followed closely by "other" businesses. Healthcare and medical providers make appealing targets to cybercriminals because they process large volumes of personal healthcare data that can be used to gain medical services, procure drugs and defraud private insurers as well as governmental benefit programs. Moreover, breaches at healthcare and medical providers have shown a pattern of inadequate security, making those operations an easy target as well as an attractive one.

Data Breaches —most common targets

TYPE OF ORGANIZATION	# OF OCCURRENCES (% OF TOTAL)
Medical	76 (25.8%)
Other Businesses	71 (24.1%)
Retail Businesses	43 (14.6%)
Financial & Insurance Services	42 (14.3%)
Educational Institutions	28 (9.5%)
Government & Military	27 (9.2%)
Nonprofit Organizations	6 (2.0%)

The biggest data breaches of the year involved a number of high-profile events that garnered significant media coverage. All of these took place over a period of time; one prominent retailer's data breach lasted for nearly a year before it was finally contained. Another retailer's breach stopped only when the retailer was alerted to its presence by a third party. In all but one of these cases, the cause of the breach was hacking. (The lone standout was an unintended disclosure of information.)

Russian cybercrime figures prominently in data breaches, especially those caused by hacking. A single group of Russian cybercriminals is suspected of perpetrating the Home Depot, Michaels and Neiman Marcus breaches, as well as major breaches at Target and P.F. Chang's in 2013. And the biggest data breach story of 2014 comes not from any individual breach, but from the discovery of one billion stolen username and password combinations and more than 500 million e-mail addresses. The trove was discovered by Wisconsin firm Hold Security, which identified the group responsible for the thefts as a gang called CyberVor ("cyber-thief" in Russian).

10 biggest data breaches in 2014

ORGANIZATION	END DATE	NO. OF RECORDS	TYPE OF BREACH
eBay	5/21/14	145 million	Hack
JP Morgan Chase	8/28/14	76 million	Hack
Home Depot	9/2/14	56 million	Hack
Community Health Systems	8/18/14	4.5 million	Hack
Michaels	1/27/14	2.6 million	Hack
TX Health & Human Services	11/25/14	2.0 million	Unintended disclosure
Staples	10/20/14	1.2 million	Hack
Neiman Marcus	1/10/14	1.1 million	Hack
Goodwill Industries Intl, Inc.	7/14/14	868,000	Hack
Oregon Employment Dept.	10/20/14	850,000	Hack
U.S. Postal Service	11/10/14	800,000	Hack

Losses such as these, and the media attention that often goes with them, have directly contributed to wider purchasing of cyber insurance in general. According to a recent survey conducted by the Ponemon Institute—a privacy, data protection and information security consulting firm—only 10% of businesses surveyed bought cyber insurance in 2013. By 2014, however, that number had gone up to 26%. Given the number of high-profile data breaches throughout 2014, the rate of cyber insurance purchases will likely be similarly higher for 2015.

Similarly, a 2014 benchmarking report by Marsh Risk Consulting noted that the number of clients buying cyber insurance rose 21% from 2012 to 2013 and that the number of clients who bought cyber policies of $100 million or more rose significantly.

This was supported by the Insurance Information Institute, which at the 2015 Property-Casualty Joint Insurance Forum polled insurance executives in attendance on a range of issues. When it came to cyber insurance, 80% of executives said they expected to see cyber insurance as a major area of growth in 2015.

THE COST OF CYBER RISK

A data breach does not have to be big to cost millions

But what are the actual insured costs of cyber losses? That is much more difficult to determine. The NetDiligence *2014 Cyber Claims Study*[1] offers some sobering information. The study focuses on 117 claims payouts for cyber incidents that happened between 2011 and 2013, for which the victims had some kind of cyber or privacy liability insurance and for which a legitimate claim was filed in 2013.

The study covers only a small subset of insured data breaches—NetDiligence estimates that no more than 10% of all cyber claims handled by insurers in 2013 made it into their study. More importantly, since many of the claims in the study are fairly recent and are still being processed, their final costs have not been determined. That said, the study does provide some eye-opening information on the cost of cyber claims and why writing this coverage is not for companies unwilling to understand this challenging market.

CLAIMS PAYOUTS.

85 claims covered by the study reported claims payouts, totaling **$62.3 million**. The average payout was **$733,109**, with the smallest claim payout being $1,000 and the largest payout being $13.7 million. The average claim payout for a large company was **$2.9 million**. The average payout for healthcare and medical providers was **$1.3 million**. What is worth noting is that the average payout decreased by 23% from the previous year's study, underscoring how cyber claims are trending toward greater frequency, if not greater severity, as more insureds are comfortable with presenting claims for cyber losses.

[1] NetDiligence is a leading provider of cyber risk management services. The NetDiligence *2014 Cyber Claims Study* covers information in 117 data breach insurance claims, as reported by ACE, AIG, Ascent Underwriting, Beazley, Chubb Group of Insurance Companies, CUNA Mutual Group, Freedom Specialty Insurance, Lockton, Hylant, Liberty International Underwriters, Marsh, OneBeacon Professional Insurance, Philadelphia Insurance Companies, Travelers, XL Group and Zurich NA. Starr Companies did not contribute to this study, and none of the study's data involves claims made to Starr Companies.

COST PER RECORD.

Of the 117 claims it surveyed in its study, 111 of them involved the loss or misuse of personal sensitive data. (The other six incidents involved business interruption losses or the theft of trade secrets.) The average cost notifying those whose information was involved in a breach, and of providing them with protective services such as credit monitoring, was **$956.21 per record**. But that only tells half the story.

In some claims, the cost per record was $0, and in others, it was $33 million. There are some losses with high numbers of breached records, with low cost per record and vice versa. Obviously, this presents a huge range of risk, but consider this: the average number of records exposed per data breach in this survey is 2,411,730. In a hypothetical claim involving the average number of records and the average cost per record, the ensuing claim would be **$2.3 billion**. This speaks to the potential of cyber claims, if not their current loss history.

CRISIS SERVICES.

Crisis costs—such as notifying victims that their information has been compromised, forensic investigations and public relations—comprised 48% of the total claims payouts for this study. The average cost for crisis services was **$366,484.**

The average cost of crisis services per claim has dropped dramatically, however. In 2011 it was $881,533; in 2012 it was $982,620; and in 2013 it was $737,473.

LEGAL COSTS.

Legal defense costs comprised only 15% of the total claims payouts for this study, but the average cost for legal defense was **$698,797**, while the average cost for legal settlement was **$558,520**.

REGULATORY COSTS.

Only six claims in the study involved regulatory costs, but those costs were significant. Regulatory defense costs averaged $1.04 million, and regulatory settlements averaged **$937,000**. What is important here is that regulatory costs do not appear to correlate with the number of records involved; some losses involved only 80 records while others involved 35 million records. The primary factor to consider here is the one most difficult to predict: the potential regulatory reaction to any given data breach.

THE STARR DIFFERENCE

Better service through information and crisis management

Starr provides cyber coverage as an all-inclusive form, without additional features from third parties attached. This is fairly unique for this marketplace, and it ensures Starr clients that the cyber coverage they buy from Starr includes all coverages in the base form.

Cyber risks are evolving rapidly and unpredictably

Because cyber risks are evolving so rapidly and unpredictably both in terms of the nature of the risks themselves and how much the cost of any given data breach costs the insurer, Starr is not aggressively seeking cyber business by writing large amounts of volume indiscriminately. Rather, Starr handpicks its cyber clients, and the coverage it offers is not priced to scrape the bottom of the market.

Starr's standalone cyber product is most commonly sought by healthcare companies and banks, and some 70% of these accounts that Starr services has some kind of cyber coverage built in, as part of a blended approach to addressing their total insurance needs. Case in point: errors & omission coverage and cyber coverage, which naturally go together in a situation where the failure of a product (such as computer security services) could be blamed for permitting a data breach to occur.

Starr's ideal cyber client ranges from $3 million to $500 million in revenue. At that size, most companies are likely to have somewhat less sophisticated approaches to understanding cyber liability, so as a result, Starr has crafted a simple, easy-to-understand policy that covers all of the base points within nine pages—less than half of what is commonplace elsewhere in the market. Starr's cyber policy covers security and privacy liability, privacy crisis expense, business interruption, data recovery, regulatory proceedings and cyber extortion. (Note that Starr's cyber coverage does *not* cover professional liability.)

Security & Privacy Liability. This covers any liability issues that arise from a data breach. This could include defending against a class action brought by irate retail customers whose credit card numbers were exposed by a data breach and who hold the retailer responsible. Or it could include legal action by a third party against a company that suffered a data breach in which sensitive information belonging to the third party was compromised.

Privacy Crisis Expense. This is one of the most in-demand aspects of Starr's cyber coverage. It covers the expenses incurred by the insured to retain certain cybersecurity services to help contain the loss. This can include forensic investigators to see how bad a data breach really is, notification services to let affected parties know about the breach, credit monitoring services for affected parties and even public relations costs to help protect the corporate reputation and brand of the client suffering the data breach.

Business Interruption. This is where Starr gets very selective in what is covered. At present, covered sources of loss include cyber issues caused by viruses, malware and denial-of-service attacks. It covers lost income, mainly resulting from such events. It is ideally suited for more sophisticated clients that can quantify their revenue lost during a cyber event.

Data Recovery. This covers the cost to restore and recover lost or damaged data. As part of this service, Starr will retain experts on the client's behalf who can determine exactly how much data was lost—which in many breaches is easier said than done. This coverage is especially useful for instances of cyber vandalism, where the intent of the breach may be more to wreak havoc than to steal or leak sensitive information.

Regulatory Proceedings. A major concern for all companies is the degree to which a data breach may subject them to certain regulatory fines or penalties. This is especially true of healthcare and medical providers, which are frequent cyber targets and which tend to have large volumes of personal health information on hand that is protected by HIPAA—the federal Health Insurance Portability and Accountability Act of 1996. HIPAA protects an individual's confidentiality and security of their personal healthcare information. Companies that fail to properly safeguard this information can face significant regulatory fines and penalties. That is where this aspect of Starr's cyber coverage comes in to cover the cost of such fines and penalties and to fund any legal defense against them.

Cyber Extortion. This covers the costs of any payouts made by the insured to a third party who has demanded a payment in exchange for any kind of cyber-related threat. (This was initially the case in the Sony cyberattack; the hackers demanded money from Sony or else they would begin releasing hacked data. Sony never paid and so the hackers began releasing data.).

The current cyber insurance market is one where the demand exceeds the supply.

Because of the strength of Starr's primary cyber form, Starr gets an influx of excess opportunities, as brokers often go to Starr to fill in the needs of its clients that cannot get the full coverage they seek elsewhere. This is not an uncommon situation, as the current cyber market is one where the demand exceeds the supply and is likely to remain that way for some time as increasing numbers of clients wish to procure cyber coverage, but at limits that are simply beyond carriers' risk appetites. Until the scope, frequency and severity of cyber risk can be better understood, most cyber policies are likely to offer very tightly controlled limits and conditions.

A value-added feature Starr offers its cyber clients is access to eRisk Hub, a Starr-branded online portal that contains a wide variety of cyber risk management reports, tools and resources. Registration is free for all Starr employees, so anyone within the company can use this to get a better understanding of what cyber risk is and where its greatest insurability challenges and opportunities lie. The eRisk Hub includes a constantly updated News section, a robust library of cyber risk White papers, reports and surveys and access to a deep roster of cyber security experts who can provide insight on the particulars of cyber liability and data breaches. Through the eRisk Hub, clients can also contact Breach Coaches, who can provide training for what to do immediately following a breach to minimize losses.

CONCLUSION

There is always another Sony

While Sony's unprecedented cyberattack made headlines near the end of 2014, 2015 quickly became the year of the healthcare hack, with numerous breaches—sometimes affecting many millions of documents containing personal healthcare information—making headlines. The changing nature of cyber risk makes this one of the most rapidly evolving insurable risks in the world today.

The kinds of exposures themselves are swiftly adapting to all efforts to prevent or contain them, thanks to criminals who are motivated to exploit any and all data architectures for thrill or for profit and thanks also to a generation of programmers who see any form of hacking as a kind of intellectual challenge.

The values at risk seem to grow exponentially, as the legal liabilities for protecting consumer data in particular show no signs of receding any time soon. Certain kinds of personal data with special legal protections raise the stakes even higher for any business touching that information, as companies have a special duty to protect it.

But there is help. Starr cyber coverage can not only provide financial compensation for the many different kinds of economic damage caused by a data breach, but Starr also provides a wide suite of robust loss control services that can help a company to recover more swiftly from a breach and to better understand how to limit its exposure to cyber risk in general. With Starr Cyber at your disposal, cyber risk can become a much more manageable risk, so you can focus on what matters most: your business.

The coverages described in this document are only a brief description of available insurance coverage. It is intended for general information purposes and does not provide any guidance regarding coverage that may or may not be available under this policy in respect to any claim. Any policy issued by Starr Indemnity & Liability Company will contain limitations, exclusions and termination provisions. Not all coverages available in all jurisdictions.

Starr Companies (or Starr) is the worldwide marketing name for the operating insurance and travel assistance companies and subsidiaries of Starr International Company, Inc. and for the investment business of C.V. Starr & Co., Inc. and its subsidiaries. Starr is a leading insurance and investment organization with a presence on five continents; through its operating insurance companies, Starr provides property, casualty and accident & health insurance products as well as a range of specialty coverages including aviation, marine, energy and excess casualty insurance. Starr's insurance company subsidiaries domiciled in the U.S., Bermuda, Hong Kong and Singapore each have an A.M. Best rating of "A" (Excellent). Starr's Lloyd's syndicate has a Standard & Poor's rating of "A+" (Strong). Starr's insurance company subsidiary domiciled in China has an A.M. Best rating of "A-" (Excellent).