CYBER INDEMNITY SOLUTIONS

WHY PROPERLY INSURING YOUR ELECTRONIC DATA AGAINST PERMANENT LOSS IS NOW CRITICAL

The Need for a High Indemnity, Broad Coverage Policy

A Cyber Indemnity Solutions Ltd. White Paper

June, 2017

WHY PROPERLY INSURING YOUR ELECTRONIC DATA AGAINST PERMANENT LOSS IS NOW CRITICAL

1. Executive Summary

In many cases, electronic data is a business' most valuable asset and simultaneously one of its largest risks. Continual advances in software allow businesses to capture more and more data about their operations, their customers and their competitors. This data is used for both routine and strategic decisions. Despite its importance many companies still do not properly protect their data and lose it. For the purpose of this paper, data is deemed to be 'lost' if there is an inability to retrieve it from its storage medium. To protect against the financial consequences of data loss, it is absolutely imperative for businesses to complete a thorough data risk assessment and implement appropriate data loss prevention measures. The April 2017 cover of The Economist stated "Why Computers Will Never Ber Safe"! The reason they state: "Computer security is broken from top to bottom" and "Everything is hackable". Recognizing this and that data can be either purposely or accidentally lost, it is good business practice to purchase data loss insurance. Cyber Indemnity Solutions Ltd. (CIS), an Australasian based Insurtech company, has developed a revolutionary Digital Asset Protection Policy to insure permanent data loss that goes well beyond traditional policies in protecting insureds from a major financial loss. CIS provides insurance companies and brokers with a complete underwriting system and training program so they can offer their clients a high indemnity, broad coverage data loss policy.

2. Data is a Valuable Asset

The use of smart meters, mobile sensors, internet connected devices and other new technologies is increasing the amount of electronic data exponentially. Companies need to store and analyze this data and then turn it into information. With data being used for almost every purpose including day-to-day operations, marketing, financial and strategic business decisions, data has become more valuable than ever to an organization. While data creation in the past ten years has been characterized primarily by an increase in entertainment content, the coming decade will reflect the shift to productivity-driven and embedded data; with critical data growing 39% and hypercritical data growing 54% (i).

The cost of cyber crime is high enough that new EU Regulations are focused on identifying systemically important data institutions – an implicit recognition of the growing importance of data valuation to firms and nations alike (ii). Statistics may vary, but there is a consensus that the loss of critical data would create severe financial consequences for any business. Given the value of data, it is essential to protect and insure it.

3. Data Needs To Be Protected

Despite the importance of data, many companies fall short when it comes to effectively managing and protecting this asset. Data resides on servers, desktops, laptops and tablets. It is located in head office computers or field tablets and can be stored in-house, outsourced to data centres, or stored with service companies. It is a challenge for companies to manage and keep secure their immense store of widely dispersed electronic data.

PWC LLP concluded in a research study of 884 public company directors that many board members are still uncomfortable with overseeing their company's IT, although 81% of them are involved with overseeing the risks of cyber attacks (iii).

The Economist stated in 2017 that "Computer security is a contradiction in terms. There is no way to make computers completely safe. Software is hugely complex. The average program has 14 separate vulnerabilities, each of them a potential point of illicit entry. Such weaknesses are compounded by the history of the internet, in which security was an afterthought" (iv). These factors make data loss prevention a huge undertaking.

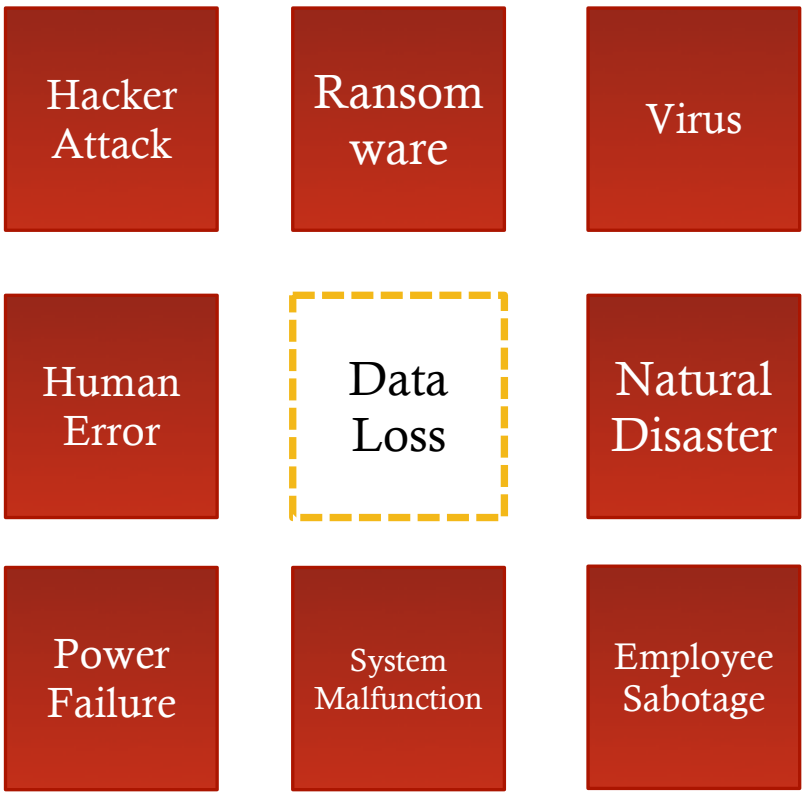
Business owners, senior management and boards acknowledge their struggle with understanding their IT strategy and many do not know whether their data resources are safe. Electronic data, like any other valuable asset, should have its own risk assessment, loss prevention and insurance purchase strategy. The strategies for data loss protection and the availability of adequate insurance coverage are in their infancy compared to the protection and insurance of other assets.

4. How Data Can Be Permanently Lost

Data can be lost for a number of reasons (lost means unrecoverable or irretrievable – not lost into the public realm such as the loss of private customer information). Hardware failures and the lack of comprehensive monitoring and maintenance plans for critical systems account for the greatest majority of data loss. Other common causes of loss include software bugs, employee sabotage, fire, flood and other perils, natural catastrophes, virus, hacking, theft and power failure.

According the the FBI, more than $209 million in ransomware payments have been paid in the United States in the first three months of 2016, up from just $25 million for all of 2015 – an increase of 3300% (v). Datto, a Connecticut based cybersecurity company found that in a survey of 1,100 IT professionals, 92% had clients that sufferred a ransomware attack in 2015. Furthermore, according to CSO, backups can also be encrypted if they are attached drives or networked, and cyber extortionists know that backups are their number one enemy and are adapting their ransomware to look for them (v).

Many insurance claims are due to two or three unexpected scenarios happening concurrently. A server crash at the head office at the same time that the offsite storage data center has a fire could result in a complete loss of data. The same result could occur in a catastrophe such as a flood, earthquake or hurricane if the backup location is too close to the original source of the data. A disgruntled employee with access to the data could also destroy multiple copies.



When data is stored in the cloud or with a service company, the data loss prevention measures are not controlled by the client. These storage sites can also experience losses. For example, in the past a huge cloud services company's servers crashed, permanently destroying data; a data services company, whose customers included Fortune 500 companies, blamed permanent data loss on the failure of 'multiple storage disks'; and a server rental company lost data belonging to 5,600 businesses following a system failure.

EMC Corporation announced the results of new research revealing that organizations are failing to appreciate the growing challenges of protecting their data and, as a result, are experiencing the economic impact of data loss. New findings from the EMC® Global Data Protection Index 2016, an independent study by Vanson Bourne of enterprise backup in eighteen countries around the world, revealed that, while businesses have been successful in reducing the impact of the four biggest traditional data loss risks, they are unprepared for new, emerging threats, which are taking their toll instead (vi).

5. Data Safety Versus Data Storage

Off-site redundancy is better than on-site because it minimizes obvious loss scenarios such as fire, theft and flood at the client site. However, it is extremely important for the data owner to set the standards for where, how and how often the data is stored off-site. Data backup services may advertise that date is mirrored twice to protect against loss but if it is all stored in the same room in a data centre, it is subject to the same loss scenarios such as fire or server failure. One company lost data because a technician

accidently set off the fire suppression system which created a sonic boom loud enough to destroy some storage raid discs.

Data centers are usually certified to one or more standards, such as SSAE No. 16 (Auditing Statement), ISAE 3402 (Global Assurance Standard) or the Uptime Institute (tiered data center rating). Unfortunately data center certification does not directly relate to data security because these ratings are more focused on uptime than on ensuring data is not lost. When working with service companies, management should receive and evaluate the loss prevention documentation.

Given that data can be accidentally lost when using a data storage or a data service company, what recourse is available? The answer is essentially none. Why? Because these data companies know that while it is possible to lose critical data, to provide any sort of meaningful financial compensation would severely damage their balance sheet.

6. Loss of Critical Data Can Be Expensive

The impact to a company from a loss of data can generally be classified as business interruption, extra expense or consequential damage. The magnitude of the loss can vary from small to bankruptcy depending on the quantity and importance of the data lost. If an organization's information were to be irrevocably lost with no chance of recovery, the impact could include lost customers,damage to the brand, decreased revenue, increased expenses and a tumbling stock prices. Loss of data can significantly impact the company, customers, suppliers, employees and shareholders.

Code Spaces was a company that offered developers source code repositories and project management services. A hacker somehow gained access to Code Spaces' AWS control panel account, then got the folks at Code Spaces' attention by mounting a denial-of-service attack and delivering a ransom note through the AWS control panel. The Code Spaces folks responded as geeks everywhere would: They started nailing down their control panel, changing passwords and the like. However, the hacker was watching them via a backdoor account he created, and when he saw them locking doors, he set off the metaphorical bomb he'd hidden in the basement and started deleting AWS objects like EC2 machine definitions, S3 buckets, and, of course, all the backups. As a result, Code Spaces lost all their data and went out of business.

Auditors and government regulatory bodies are becoming increasingly interested in the process and standards employed by companies regarding the safe keeping of their data. Auditors that want to know the risk impact of the loss of a large customer on corporate profits now also want to know the risk impact of the permanent loss of departmental data. Governments are also becoming more interested in data security from a tax and company survival point of view, especially if the company is in a regulated area such as the financial services sector.

7. Steps to Mitigate Data Loss

There are five steps that a company can take to prevent the loss of data and to mitigate the financial impact if data is permanently lost. These steps are similar to the method companies currently use to mitigate the loss of other valuable assets:

1. **Document** - what data is stored, where and how often the data changes
2. **Determine Cost Impact** - calculate the cost impact if data is lost by data groups such as department, device or location

3. **Risk of Loss** - review the potential for the data to be lost, since different data can be stored or accessed in different ways
4. **Loss Prevention** – implement improved data redundancy, encryption, access rules
5. **Insurance** – purchase policies that protect the company from significant financial hardship

Step 1, Document, is the first step in the creation of a risk management strategy. Perhaps the most difficult one is step 2, Determine Cost Impact. In this step, it is important for companies to calculate both the cost and profit impact of losing data. For example, the cost of restoring financial data could include the cost of hiring additional staff and invoices from auditors, accounting firms or suppliers. Step 3, Risk of Loss, is determined by such factors as who has access to the data, firewalls, redundancy, login protocols and storage mediums.

Step 4, Loss Prevention, addresses the risks identified in the previous step. Additional redundancy, although not a complete answer, can be accomplished using a variety of mediums: tape, USB stick, disc and through a variety of methodologies: on-site duplication, off-site courier service or an on-line internet service. With each protocol, it is important to evaluate the effectiveness of the backup relative to security, retrieval time and time lapse between backups. Step 5, the Insurance Purchase decision is not easily made unless one decides that like other insurance purchases for property or liability, the decision is a 'must do' in order to protect the finanicial viability of the organization in case of the fortuitous loss.

8. Insuring Against the Permanent Loss of Data

Insurance companies currently do provide some coverage against total loss of data as part of a property, cyber or equipment policy. Company management should review each of their policies to determine how much coverage is provided, and for what types of accidents. Property policies should provide some data coverage against loss from insured perils; equipment policies should provide cover for accidental breakdown; and cyber policies should cover for hacking, viruses or malicious damage. Management should also review what costs are paid for in case of a data loss. Does the policy respond only to payment for extra expense such as re-inputting the data, or does it also compensate for lost revenue?

Unless the insurer has undertaken a special underwriting review, the data loss indemnity is often sub-limited to a value much less than the policy limit and also much less than the true cost impact of losing the data. In addition, the claim payment is most often only for the restoring or retrieving of data – which in today's world most often cannot be done because the data does not exist in other places. It is quite expensive for an insurer to conduct a risk assessment to offer an indemnity that is meaningful. To do so means knowing what data is insured, the value of the data, how it is protected, whether the standards of protection are constant, how frequently data is lost and what scenarios would result in a catastrophic loss.

9. The CIS Digital Asset Protection Policy

To overcome the challenge of insuring data against permanent loss, Cyber Indemnity Solutions Ltd. (CIS) developed a new underwriting concept that allows insurance companies to offer high indemnity, broad coverage insurance to compensate data owners for the cost or profit impact if data is permanently lost. Successfully operating for several years, the Digital Asset Protection (DAP) policy and storage system combines advanced global data security protocols and loss prevention procedures with auditing requirements. CIS is an insurtech licensing company that provides policy wordings, sales training,

proprietary software, underwriting, reinsurance and claims adjusting to insurance companies and syndicates. The DAP policy wording can be sold on a stand alone basis or be embedded into property, cyber, equipment and D&O liability policies. It can also be offered a part of a data backup product or IT service to provide the end user with a financial guarantee in case of a permanent data loss.

With the DAP policy, after the insured determines the desired indemnity, the data is automatically insured as soon as it is mirrored to an underwriter approved data storage service. Indemnification is provided if mirrored data cannot be returned to the insured or via data restoration (the polciy has more details).

With this new methodology and policy wording, businesses are finally able to insure their data against accidental loss for limits that extend into the millions of dollars and for loss scenarios that were previously not covered. The benefits of purchasing a DAP policy goes beyond employing best practices, corporate governance and protecting the financial stability of the business. CIS also provides the buyer with the assurance that the data storage company is providing the best protected storage service possible. This is a huge benefit, especially for most small to medium sized businesses, because it can be difficult for management to adequately perform a comprehensive risk assessment on a data service, and to be confident their company is not at risk if there is a permanent data loss.

10. DAP Policy Mechanics Overview

a. The insured determines what critical data needs to be insured. For smaller companies, this might be all of their data. For larger enterprises, this can be accomplished in-house or with assistance from a CIS Crimson Risk partner.
b. In the situation where the DAP coverage is embedded in another policy, the indemnity level will initially be specified, with the option to increase the level. For an enterprise monoline policy, the insured can choose an indemnity level for each data segment. CIS provides a 'data loss value calculator' to assist with this process.
c. The enterprise client can then choose to either purchase one policy with a certain indemnity level, one policy that allows segmentation at different indemnity levels for different data sets, or the insured can purchase several policies, one for each data set.
d. In case of a claim, the DAP policy also allows the settlement clause to vary dependent on the nature of the data. For example, for random data, the claim payout can be structured so that if 30% of the data is subject to data loss, then the payout would be 30% of the indemnity level. If the data is such that any loss would make the entire data set useless, then a 100% claim payment can be chosen if any data is subject to data loss.
e. Once the options within the DAP policy are chosen, the policy will be activated once the data to be insured is stored with the CIS insured data platform (IDP). This is to ensure that the insurer knows what data is to be insured, and how it will be protected.
f. All the data stored within the IDP is encrypted so that it is not accessible to either CIS or anyone else.
g. The Insured Data Platform (IDP) is a Platform-as-a-Service, (PAAS) implementation that enables data from any source (backup application, enterprise, mobile, web application and other) to be stored in a known, very secure method that takes into account all known human and cyber risks to mitigate risk accumulation.

h. The policy itself has very broad coverage, so that all accidental, malicious and external cyber threats are covered. The policy does exclude war and radiation as usual. There are temporary exclusions in the policy that are within the control of the insured – for example, if the insured changes its operating system and cannot upload data from the IDP, then no claim can be made until the operating system is changed.
i. A claim can be submitted any time that the insured is unable to retrieve data from the IDP. It is then incumbent on CIS and the insurer to provide the insured with the data. From past experience, this happens from time to time due to several reasons. CIS will assist the insured with retrieving the data. If all the data cannot be retrieved, then the insurer will provide a claim payment.
j. Further information on the policy is provided in the next section where the DAP policy is compared with permanent data loss coverage typically found in the market today.

11. Policy Comparison

Let's compare the wording for permanent data loss in a well known cyber policy and compare it to the Digital Asset Protection policy. (NOTE: Refer to the complete policy wording to make any insurance policy purchase decisions).

I. A well known 'Cyber Policy' provides the following policy wording:

A. System Damage

We agree to pay on your behalf **rectification costs**, subject to our prior written agreement (such agreement not to be unreasonably withheld), which you incur:

a) In retrieving, restoring or replacing any of your computer programs or any other data (or any other computer programs or any other data for which you are responsible) that you first discover during the period of the policy have been lost or damaged; or
b) In repairing, restoring or replacing any of your **computer systems** that you first discover during the period of the policy have been lost or damaged.

B. System Business Interruption

We agree to reimburse you for your reduction in profit during a **system outage period** as a direct result of a **cyber peril** first discovered and notified to us during the period of the policy. We also agree to pay costs and expenses on your behalf.

C. Computer Crime

We agree to reimburse you for loss first discovered and notified to us during the period of the policy as a direct result of any third party committing;

a) .....
b) any fraudulent manipulation of electronic documentation

Definitions

"Computer Systems" means all electronic computers…..and any data or websites wheresoever hosted, including cloud computing providers, off line media libraries and data backups and……

"Cyber Peril" means any hacking attack, virus or malicious damage that adversly affects the availability of your computer systems or a cloud computing provider's systems.

"Rectification Costs" means those costs that you incur as a result of the use of external consultants, contractors or advisors or any additional costs that you incur to pay your employees. For the avoidance of doubt, rectification costs do not include any hardware costs, basic salaries of your employees…..

"System Outage Period" means the period during which you computer systems….are unavailable …..as a direct result of the cyber peril. The maximum system outage period is as stated in the Schedule.

Exclusions

Uninsurable Fines: We will not make any payment on your behalf for any claim…for fines, penalties, civil or criminal sanctions, punitive or exemplary damages, unless insurable by law.

II. Cyber Policy Analysis

This policy will pay the cost of external consultants or other costs for the repairing/restoring/replacing or retrieving (the 4 R's) of data (as part of the definition of 'computer systems') subject to the limit or sublimit in the Schedule.

It will also pay for the 'reduction in profit' during a 'system outage period' due to a 'cyber peril'. Because 'system outage period' refers to 'computer systems', and 'computer systems' means 'any data', then if 'any data' is unavailable due to a hacking attack, virus or malicious damage', then the policy will respond and pay for the reduction in profit, but only during the maximum system outage period stated in the Schedule.

To be complete, there is also coverage for financial loss sustained due to the fraudulent manipulation of electronic documentation commited by a third party, but this coverage refers to the intent to deceive or a dishonest action – not the permanent loss of the data or document.

Let's assume that a business loses its critical data (operational, mailing, and /or financial) due to an accidental mistake by one if its employees and as a result, if it does not able to restore the lost data, its income will be reduced by an average of 50% for two years.

A) Data Recovery

The issue in today's electronic world is that most data cannot be retreived / restored etc because the majority of the data does not exist anywhere else. Hence, the business might be able to recover / restore some of the data and obtain coverage from the policy – but the majority of the data is lost forever. Hence, even though the policy does pay to recreate data – it is unlikely that the insured can actually recreate the

data and continue business as normal. It should also be noted that the policy states that rectification costs are subject to "written approval" – it is unknown why this clause is inserted into the policy.

B) Business Interruption

The Cyber Policy does provide coverage for business interruption costs, but an accidental mistake is not a covered cyber peril. If the permanent data loss was due to a covered peril such as a malicious act by an employee, then the policy would respond – but only to the extent of the 'maximum system outage', which is unlikely to be 24 months. Furthemore, if the data loss was due to an equipment issue, natural diaster or power failure - then the business interruption coverage would also not respond. In other words, the business interruption coverage in the policy is limited and would not make the insured whole for most permanent losses of data. The insured is also required to prove any reduction in profit loss - which is standard in the insurance industry but for some insureds, is a huge cost and time concern.

C) Consequential Losses

In addition, if the data loss resulted in a consequential loss such as a fine by a regulatory body (such as not complying with a statuatory filing), then the amount of the fine would also not be covered by the policy.

D) Change in Conditions from Application

Another point of uncertain concern is whether the insurer will pay a claim if the insured has changed any of its IT standards as answered in the application. In particular, the application asks:

Do your internal IT systems comply with all our minimum security requirements detailed below:

i. Anti-virus software must be installed…
ii. Gateways must be protected by a firewall
iii. All critical data must be mirrored on at least a weekly basis
iv. All backups should be stored in a secure location offsite or in a fireproof safe
v. The integrity of all backups should be verified on at least a monthly basis
vi. Do you have a Service Level Agreement in place with all outsourcing suppliers

If the insured, or the supplier, stops one of the security requirements, and it is not reported to the insurer, is that then a 'circumstance which may give rise to a claim' and could result in the insurer 'not be liable for that portion of the claim…'? Do SME insureds have the time and resources to remember all these factors to ensure that they are covered when making a change in their IT systems?

III. Digital Asset Protection (DAP) Policy Wording:

The DAP policy takes a modern, broad coverage approach to insuring data against permanent loss for three reasons:

- The insured is covered for any data that they backup to the CIS Insured Data Platform (IDP) – which is easy to do
- It is a fixed indemnity policy – so the insured chooses the value of the data since they know best the financial ramifications of any data loss
- If the data cannot be retrieved from the IDP or restored in any other manner, then the policy will pay the agreed indemnity according to the settlement clause.

The policy wording states (only certain portions of the policy are referenced):

A. Basis of Settlement

a. In the event of a total **Data Loss**, the Limit of Indemnity

b. In the event of a Partial Data Loss, the payment shown in Endorsement A (this varies from pro rata to 100% of the limit depending on the importance of the data)

B. Definitions

a. Data Loss: shall mean the loss of Data from the Insured Data Platform that

i. has been previously mirrored and confirmed in the file register or record Log to the Insured by the Insured Data Platform during the policy period subject to file version control

ii. … is unable to be returned by Data Retrieval no later than twenty days following a written request by the insured….

iii. is unable to be returned by other data restoration services…

b. Insured Data Platform shall mean 1) the Insured Data Platform that stores copies of Data, 2) the Insured Data Platform Management System that enables the Insured to store copies of Data and to retrieve Data in accordance with the instructions and protocols provided to the Insured and 3) any related instructions and protocols provided to the Insured

C. Exclusions

i. War

ii. Data that is not included within the Record Log

iii. Radiation

iv. The insured not knowing their encryption key, password or user name

v. …physical loss or performance issues related to the insured's designated computer

---

IV. DAP Policy Analysis

Again, let's assume that a business loses all of its critical data (operational, administrative, financial) due to an accidental mistake by one if its employees and some sort of catastrophe at the IDP - and as a result, if it does not restore the lost data, its income will be reduced by an average of 50% for two years.

When it purchased the DAP policy, the insured used the CIS 'Data Loss Value Calculator' to determine that due to lost customers, brand damage, and the cost of contacting auditors and other suppliers to recreate lost critical data, its profit over the next two years would still be impacted by $4,500,000.

In the DAP policy case, because all the data is lost and cannot be retreived from the IDP or other sources, the policy would pay the limit of $4.5 million. In another scenario for example, if the insured had stored 100 GB's of data on the IDP, and 60 GB's were permanently lost, then the policy, depending on the chosen settlement clause, would pay anywhere from 60% to 100% of the $4.5 million limit.

For clarity, the DAP policy will not respond to data that is not stored in the IDP. The policy will also not respond in situations where the insured has, for example, lost all their password / user information and as such, neither the insured or CIS can access their stored data.

12. Conclusion

Data is one of the most valuable assets of a company. Senior management and business owners need to increase their knowledge about how to best protect and insure their electronic data against sudden and accidental loss due to the fact that cyber criminals are more adapt at stealing or detroying data then companies can protect data. After a risk assessment is completed and loss prevention measures are installed, insurance should be purchased for critical data to provide finanical compensation in case of the unexpected accident or criminal catastrophe. Cyber Indemnity Solutions enables insurers and their brokers to easily provide data loss insurance coverage that goes far beyond most current coverages and indemnities.

References:

i. Reinsel, Gantz, Ryding, 2017, "Data Age 2015: The Evolution of Data to Life Critical"
ii. Disparte, Wagner, 2016, Harvard Business Review, "Do you know what your company's data is worth"
iii. PricewaterhouseCoopers, October 2016, "Board governance in the age of shareholder empowerment"
iv. The Economist, Leaders section, April 2017, "The myth of cyber security"
v. Korolov, May 2016, CSO, "Will your backups protect you against ransomware?"
vi. EMC, 2016, "Global Data Protection Index 2016"

Cyber Indemnity Solutions (CIS) has established a global standard for insured data protection by combining insurance risk management practices, data storage methodologies and auditing procedures. CIS is an insuretech intellectual property licensing company that provides all the necessary policy wordings, sales training, underwriting, reinsurance and claims adjusting to insurance companies interested in participating in the sale and distribution of its digital asset protection policy. CIS is not an insurance company, and will refer brokers, data owners and risk managers to insurers that provide the CIS policy.

Contact Details

Cyber Indemnity Solutions Ltd.
Hans A. Schols
hans.schols@cyberindemnitysolutions.com
+1 416 505 3591

Important Notice

Information in this document was current at the time of preparation but Cyber Indemnity Solutions Ltd. gives no warranty that the product or industry information has not changed.