

DATA LOSS PREVENTION AS A CRITICAL COMPONENT OF CYBER INSURANCE STRATEGY



Executive Summary

The entire global market is changing for the better with technological and digital disruption in almost every sphere of life. On the flip side, however, it is also helping cyber attackers have a field day with multiple new avenues opening up for gaining access to business-critical data of organizations. Additionally, organizations also face loss of data internally – from within. To deal with all this and more, most organizations are opting for cyber insurance to prepare themselves for any such incidents.

This white paper discusses the types of internal threats that North American organizations need to be aware of, along with how these risks can be mitigated. This paper also examines on the effectiveness of cyber insurance in addressing challenges posed by data loss incidents and how data loss prevention solutions comprise a critical component of any cyber insurance strategy.

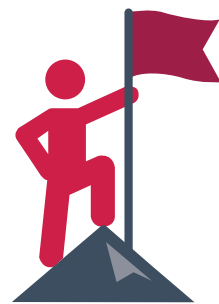


INTERNAL THREATS ARE VERY MUCH REAL

The Enemy Within

The enemy, for most organizations, lies, and thrives, within their own internal boundaries. No matter how robust and agile a system, however efficient an organization's policies and regulations, or however secure the network connections, there is always a huge and omnipresent risk of data loss - either maliciously, or due to human error or system glitches. Losses after a data-loss incident include both measurable and intangible elements including (but not limited to) direct loss of money (towards lawyers, investigators, various fees and penalties, IT forensics experts, etc.) or more indirect losses (loss of consumer faith and credit worthiness, reputation, image, etc.) - all of which can be enormous.

A lot of times, these risks and threats are internal. Internal threats for organizations may branch out from any of its departments - production, sales, marketing, or engineering. One of the most common forms of internal threat involves sharing of proprietary information about a product with competitors - this may be malicious, or due to inadvertent behaviour. Another risk involves the competency of the employees. For example, someone writes a single line of code (again, deliberately, or by mistake) that deletes or corrupts the entire file system of an organization - the impact of which can be disastrous.



"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

~ Sun Tzu.

Who Comprises Insider Threat?

Internal threats that any organization may face generally involve people. These people may include:



Employees who may, by pure chance, spill coffee on the server machine, or open an email attachment that is infected by virus (sometimes very deadly), install unauthorized software that may capture vital information and pass it on, or casually pass on sensitive information to friends etc. over a cup of coffee.



Unhappy employees who maliciously want to cause damage to avenge a wrong done to them by the management or the enterprise.



Selfish employees whose only motive is personal gain – even if it includes causing collateral damage.



Employees who perform such deeds under pressure – for example, they are blackmailed by someone to either steal critical data or damage critical IT resources or information.

The challenges to prevent data loss are tremendous but it is imperative to improve our methods to mitigate and avert the theft of sensitive data by an insider. With technological advancement, vulnerabilities to sensitive data are on the rise. Therefore, accordingly one has to come up with efficient and effective solutions to stop data loss. With increasing incidents of data breaches, it is even more essential to adopt the latest solutions and methods for data loss prevention (DLP).



The Extent of Vulnerability is Extreme

According to Vormetric's 2015 Insider Threat Report, a whopping 93% of US organizations believe that they are vulnerable to insider threats, and plan to increase or maintain what they spend on information technology (IT) security and data protection.

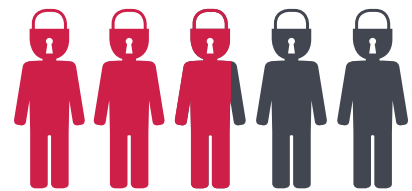
The extent of vulnerability can also be gauged by a Harris Poll of more than 800 senior business managers and IT professionals, in which 55% respondents said that their "privileged users" pose the biggest internal threat to their corporate data, followed by contractors and service providers (46%).

Most complaints investigated by the Office for Civil Rights (OCR), involve malicious, or unintentional information disclosure by employees. These also include the +50% breaches by means of backup tapes, data being transferred via mobile devices, or laptops being lost or stolen, or someone being careless enough to leave the server room unlocked, or writing down passwords in areas that are very visible.



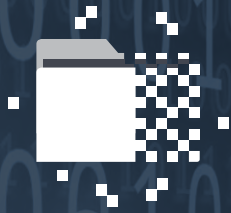
93%

of US organizations believe that they are vulnerable to insider threats, and plan to increase or maintain what they spend on information technology (IT) security and data protection.



55%

respondents said that their "privileged users" pose the biggest internal threat to their corporate data, followed by contractors and service providers



DATA LOSS PREVENTION IS CRITICAL

DLP solutions enable detection and prevention of unauthorized use and transmission of sensitive and business-critical information outside the organization's network by end users.

In today's world driven by megatrends, the reasons that necessitate the implementation of a strong DLP solution are:



Consumerization



Cloud computing



Cybercrime, and



Internal threats

DLP solutions can be set to identify, monitor and protect data in use, data in motion, and data at rest. Generally, organizations use network-based monitoring/scanning tools that scan the network/hosts/shares to identify/report/quarantine unprotected data. However, although these can be deployed very fast and cover the entire internal network, they are not so effective when it comes to scanning encrypted data.





Data Loss Can Happen Anytime, Anywhere

The probability of data loss happening within organizations is higher today than ever before. A few specific categories of data loss include sensitive or embarrassing information being exposed or transferred via emails etc., theft or exposure of information related to customers' intellectual property (IP), or confidential, sensitive, or private information via mobile devices or storage media.

According to the 2016 Internet Security Threat Report (ISTR), the number of publically disclosed data breaches has risen steadily over the last number of years to reach 318 in 2015. That is, of the data loss incidents that we know, the occurrence rate is almost 1 incident per day. Also, of all the breaches that happened in 2015, there were 10 mega breaches with an estimated financial impact of almost \$429 million.

Considering that there is an almost 85% rise in the number of breaches where the number of identities exposed was not reported, the impact definitely must be much higher. Per estimates, almost half a billion identities were exposed in 2015.



10 mega breaches reported in the last year with an estimated financial impact of almost

\$429 million



85%

rise in the number of breaches where the number of identities exposed was not reported

Taking Proactive Measures to Prevent Data Loss is a Simple, Secure, Successful Insider Threat Mitigation Strategy

Organizations today are investing a lot of money and effort for preventing data loss and on monitoring and protecting sensitive data. Following are a few measures that can be adopted:



Implement data loss prevention solution: Implement an Enterprise DLP solution rather than a piecemeal solution as the former performs both content inspection and contextual analysis of data that helps address the risk of data leaks more efficiently.



Define specific policies: First and foremost, specific policies must be defined for handling company proprietary and business-critical information. Employees must be asked to sign non-disclosure agreements (NDA) indicating acceptance of their responsibilities.



Document access rules, roles, and functions: Assess and identify roles and functions that can access confidential information, and have a document that defines the terms and conditions for initiating and terminating such access. This helps in damage control from terminated, disgruntled employees whose access to information is not cut off in a timely fashion.



Track access: Keep a tab on employee activity to ensure that they are not misusing their access rights. This helps to identify any risks early on and also initiate any mitigation plans.



Be vigilant: Ensure proper vigilance in your organization to understand the causes of lapses of privacy incidents, provide mitigation facilities, etc.



Provide frequent training: Provide training related to the perils of cyber attacks and the need for proper management of information and security at frequent intervals. This helps employees understand what they need to do in situations where they have unauthorized access or unintentional exposure to protected information.



Penalize the violators: Create a provision for proper penalties and fines against invasion of information privacy or security violations. In absence of such provisions, organizations are bound to suffer financial and reputational damage.



Scan data being shared: Perform local scanning and real-time monitoring of databases, network file shares, and other enterprise data repositories for confidential data being accessed, downloaded, and transferred to or from laptops and desktops, including through email or cloud storage.



Don't forget checking the devices: In the more contemporary context, include iOS and Android devices under the monitoring provision for data loss prevention.



CYBER INSURANCE ACTS AS A COVER TO DEAL WITH THE AFTERMATH

Cyber Liability Insurance Cover (CLIC) policies provide safety against losses that arise due to cyber attacks such as hacking and denial of service, data loss (by means of theft or extortion), etc. The liability coverage provided indemnifies organizations for losses caused to others by means of failure to save data loss, defamation caused due to data exposed, etc. The benefits of cyber insurance include security audits on a regular basis, expenses that cover post-incident PR and investigations, and criminal reward funds. Cyber insurance, thus, acts as a hedge against risks linked with the loss of customer data, which can leave a really huge dent to an organization's finance and reputation.

In brief, cyber insurance is an insurance product that helps protect organizations from risks related to information technology infrastructure and activities.

Security solutions play a critical role in today's world where cyber attacks show a rising trend. Security related services have thus become an integral and essential part of the strategies being developed for protecting the confidentiality of data related to government, public, healthcare, military, BFSI, and other businesses. Organizations across sectors – large, medium or small – therefore, are queuing up to buy cyber insurance as a measure of protection against the financial losses related to data loss and business disruption.



Security solutions play a critical role in today's world where cyber attacks show a rising trend. Security related services have thus become an integral and essential part of the strategies being developed for protecting the confidentiality of data related to government, public, healthcare, military, BFSI, and other businesses.

DATA LOSS PREVENTION AS A CRITICAL COMPONENT OF CYBER INSURANCE STRATEGY



In the US, 46 states have made it a law that data breach incidents be notified publicly - resulting in exponential demand for cyber insurance. Although 90% of the global cyber insurance policies are bought by US companies, yet only one-third of the US companies are covered.

This is enough justification for companies – large, medium or small – to get Cyber Liability Insurance Cover or CLIC. Of course, the coverage will not be the same for all but has to be customized as per the entity and therefore will have various terms and conditions and pricing. The major factors that dictate the type of CLIC are the type of data aggregated, size of the company and extent of the potential risk.

Cyber insurance companies offer add-on services with CLIC to custom build policies for organizations. Be it lawyers, forensic experts, spend on crisis management solutions, notification and restoration expenses – all become an intrinsic part of the coverage.



60%

In 2015, about 60% of brokers said that the number of organizations researching and opting for cyber insurance in 2015 increased significantly, thereby leading to a greater demand for DLP solutions.

DATA LOSS PREVENTION AS A CRITICAL COMPONENT OF CYBER INSURANCE STRATEGY

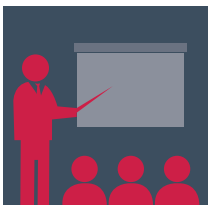
Cyber insurance companies that provide the best fit will typically have the following elements covered as part of their packages:

- First party as well as third party coverage
- Premium pricing
- Claims payout
- Underwriting risks
- Ability to offer coverages (policies, term and conditions) over a wide spectrum of cyber risks which include theft of intellectual property, data and software loss, network failure liabilities, data destruction, DoS, etc.

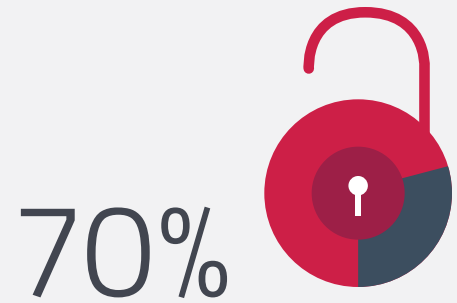
Similarly, underwriters at cyber insurance companies look for the following factors while setting premium rates for CLIC:



Check if DLP solutions are implemented. Also check for types of encryption, security for access points in the system. A comprehensive DLP solution could typically result in lower risk and hence lower premiums.



Understand awareness level of employees around access policies. This includes checking if regular trainings are held to keep employees updated on systems and policies in place. How well educated employees and vendors are about regulations and compliance has a significant bearing on CLIC.



70% Additionally, more than 70% of CLIC sales were a direct result of the newly generated interest and awareness about data breaches.



Check what risk mitigation plan is in place in case of a data breach incident.

As in the case of any traditional insurance, if there is a rise in the number of claims and payouts, the CLIC deductible and premium increases. Or, the payout is cancelled completely when capped. As a result, organizations looking for CLIC usually demand more comprehensive DLP solutions. When an underwriter sees and is convinced that the organization has taken good measures to prevent data losses, it may result in lower deductibles and premiums.

DATA LOSS PREVENTION AS A CRITICAL COMPONENT OF CYBER INSURANCE STRATEGY

According to a survey conducted in early 2015 by Veracode and NYSE, 91% of 276 companies said that they had bought cyber insurance to cover for instances of data restoration and business interruption. Almost 54% indicated that they also bought cover for expenses such as PCI fines, breach remediation and extortion. for example. The study revealed that 52% of organizations buy cover to tide over losses incurred by data stolen by employees, while 35% buy cover against loss of business-critical data that may be caused by software coding and human errors.

In addition to the above, there are various other reasons that are driving sales of cyber insurance:



Regulation:

46 states in the US have made it a law that data loss incidents must be notified publicly resulting in exponential demand for cyber insurance.



Risk transfer:

Cyber insurance acts as an important risk transfer mechanism by helping insured organizations share the cost of incidents amongst themselves. Considering that usually all policyholders will not incur losses together in a single year, when multiple policyholders pay the premium, the risk gets spread evenly across the insured organizations.



Offset Costs:

Cyber insurance provides credit monitoring facilities and also helps with the notification costs to organizations and individuals affected by the breach. It additionally contributes towards the legal costs to help understand the complicated statutes and penalties, and also for understanding (via forensic research) the data affected by the breach. This helps organizations financially in case they are sued for the breach.

DATA LOSS PREVENTION AS A CRITICAL COMPONENT OF CYBER INSURANCE STRATEGY



Best security policies:

It motivates customers wishing to be insured to follow the best practices available in the world of cyber security. An organization that clears the certification audits related to recommended practices becomes eligible for getting insurance at better rates.



Number of cyber incidents:

The recent increase in cyber incidents, both in number and severity, including a string of high-profile hacks and data breaches.



Newer security standards:

Today, a number of US Government bodies such as the NIST Cyber security Framework, the Terrorism Risk Insurance Act (TRIA), the New York State Department of Financial Services, etc. are creating new standards that support and promote cyber insurance, which, in turn, helps protect organizations against security breaches.

CONCLUSION

PwC predicts that “Cyber insurance market will grow to an estimated \$7.5 billion in annual premiums by 2020.”, and Allianz Global Corporate & Specialty, a German insurer, foresees that cyber insurance premiums will grow globally from \$2 billion per year to \$20 billion by 2025. This will be a driving force in putting forth better policies and measures for DLP in companies.



Wrapping up, embracing cyber insurance is no more a choice, but rather a need that will help organizations brace themselves against the monumental payoffs otherwise faced in case of data breaches. While the environment is conducive for the creation of a robust cyber insurance market, there still are quite a few dark corners that need to be researched and addressed for it to stabilize, and grow. Thus, frequently reforming and revisiting the current policies and then trying to implement them for better and more effective DLP solutions is a business-critical need of organizations to keep cyber insurance related costs under control.



ZECURION - THE FULL DATA LOSS PREVENTION EXPERIENCE, WITHOUT THE FULL DLP PRICE

Zecurion data loss prevention (DLP) solution is an easy-to-use solution for securing confidential data at rest, in motion, at the endpoint or on network, in the cloud, and to demonstrate regulatory compliance. With pricing and configurations that are SMB as well as large-enterprise friendly, Zecurion DLP is quick and easy to integrate into the existing IT infrastructure without any complexity. The solution supports network, endpoint and agent-based discovery functions. Zecurion is continuously developing technologies including those addressing risk of leaks through social and mobile applications.

Zecurion Enterprise DLP for End-to-End Protection

-  Zgate (Traffic Control)
-  Zlock (Device Control)
-  Zecurion Zlock Mac
-  Zserver (Storage Security)
-  Zdiscovery (Discovery)
-  Zecurion Mobile DLP

Zecurion's DLP System Manages Complexity

Making it simple to use for small to large enterprises

Regulatory Compliance

Support & Training

Simplicity of Acquisition and Implementation

Easy and Intuitive to Use

Fast Response Time (1-2 Months, From Feature Request to Delivery)

Scalable

Price Sensitive

No Restriction On Endpoints that can be Secured

Modular Architecture that Provides Reliability, Scalability and can also be Adapted to Meet Complex Deployment Scenarios

Single Management Console with Graphical Reporting



About Zecurion

Global innovator & leader in security solutions that reduce risk by addressing internal threats

Zecurion has successfully developed and implemented security solutions providing proven and reliable protection against leaks for thousands of companies around the world. Started in 2001, this privately held company was one of the first to bring to the market highly sensitive, robust products enabling organizations to manage the risk of employees accidentally or intentionally sharing confidential information.

In addition to DLP solutions, Zecurion is expert in cryptography, and a leading provider of encryption to protect data during storage and transfer. The company's solutions provide comprehensive protection against the leakage of information throughout the course of its lifecycle – from creation and recording to archiving and deletion. Its product suite and integrated platform is easy to deploy – simple administration set up and policy

selection – and easy to manage – with an intuitive console that can easily be customized. Zecurion is continually developing solutions including those addressing risk of leaks through social and mobile applications.

Zecurion is a global company with headquarters in Moscow and New York, and representation in Eastern and Western Europe, providing services to over 10,000 small and medium businesses as well as large global enterprises.

Zecurion has been recognized by Gartner in the 2013 and 2016 Magic Quadrant for Content-Aware Data Loss Prevention. It has also received recognition through the prestigious Golden Bridge Awards and Network Products Guide, as well as consistently ranked highest among developers of DLP Analytics by CNews.

www.zecurion.com

14 Penn Plaza, 9th Floor, New York, NY 10122

(866) 581-0999

info@zecurion.com

Contact Us

