Computer Science and Information Technology 5(1): 1-7, 2017 http://www.hrpub.org
DOI: 10.13189/csit.2017.050101

Technological and Information Governance Approaches to Data Loss and Leakage Mitigation

Amie Taal[1,*], Jenny Le[2], Alex Ponce de Leon[3], James A. Sherer[4], Karin S. Jenson[4]

[1]Deutsche Bank AG, New York, New York, United States
[2]Fronteo, New York, New York, United States
[3]Google, Mountain View, California, United States
[4]BakerHostetler, New York, United States

Abstract While foreign national cyber-attacks tend to garner headlines, organizations should also consider "Data Leakage" incidents caused or perpetrated by insiders, whether intentional or otherwise. But addressing Data Leakage is especially tricky because of two integral aspects that require a nuanced approach to finding a solution: (1) Data Leakage is a problem that often affects organizations *within* their firewalls. Data Leakage therefore presents a conundrum where employees are both the potential creators as well as the potential solution(s) to an insider threat. Solutions to this conundrum present a challenge where strictly adhering only to an existing policy diminishes an organization's otherwise beneficial ability to react to rapidly changing environments. But organizations are not naturally policy-driven, as the vast majority of employees—and data transfers—are not puppets of an omniscient author. So, while a perfect policy with perfect application (by perfectly informed employees) would be the best solution, that panacea simply doesn't exist. (2) While Data Leakage *can* be malicious in nature, malicious intent need not exist. Most employees and data transfers are not solely policy driven (and therefore cannot be treated as such in service of their jobs). Instead, many—if not most—potential Data Leaks will be perpetrated by people accidentally or guided by malicious direction or incompetence. Considering the duality of roles employees play in Data Leakage and that the hazardous outcomes are often accidental, we conclude that strict policy adherence is neither feasible nor available. Instead, a partially directed, partially improvisational approach is an appropriate means by which an organization can consider and address Data Leakage issues associated with Insider Threats.

Keywords Data Leakage, Data-at-Rest, Data Loss Prevention, Employee Incompetence, Malicious Insiders

1. Introduction

Data loss prevention (or DLP strategy), focused on Data Leakage, may be considered through the two "I" core concepts of Data Leakage. First, an examination of the *Inside*, which considers how Data Leakage presents "Inside the Firewall." Second, considerations of *Intention*, where Data Leakage may happen through the actions of an innocent party (or patsy) directed by a malicious party or simple mistake or incompetence that is not directed by anyone.

A convincing strategy proposal should begin by defining the issues at hand. We incorporate by reference the four-part definition of data loss previously adopted by Taal et al. [1] The first part details organizational considerations aimed at preventing intrusion into the corporate network and internal unauthorized access. These considerations account for the organization's strategy and historical efforts, which may include firewalls, intrusion detection systems, internal monitoring systems, and some combination of data loss or "leakage" prevention (DLP) efforts [2], which may include both intrusion detection systems (IDS) and intrusion prevention systems (IPS).[3] The second part, and perhaps the most common approach, incorporates two core concepts of data loss: *Data Leakage*, or those instances where sensitive data is no longer within the organization's control [4], and *Data Disappearance* or *Damage*, where "a correct data copy is no longer available to the organization."[5]

In order to appropriately consider the concept of data loss and its prevention—or, at least, its mitigation—we must address how a given corporate environment both prevents and encourages Data Leakage. This is the crux of modern information technology, where within an organization's firewall; data transfer and connectivity are not discouraged but rather supported. This is axiomatic; throttling connectivity within a collaborative environment, even in the service of greater data security, can create an inadequate computing infrastructure, cripple data transfer performance, and impede organizational progress. [6]

In a world where every system of value may be compromised [7], the third consideration affecting our analysis arises: the additional ramifications of data loss when an organization is informed of a loss (that is, "caught") or self-reports, which in turn requires a determination of how data loss is defined by statute—including the measure of the loss—as disclosure laws differ from state to state, country to county, and even by region. [8]

While this definition thus far incorporates what actually happens during an event and the legal and regulatory consequences that follow, it has yet to account for the fourth and final part of the model: the perspective of the other people to whom the data loss may matter. This may include various stakeholders, some of whom are the business people reliant upon the information and the information technology professionals who support that work but also, by extension, the organization's other employees, lawyers, and sometimes even customers and third-parties (particularly in those instances of protected health information).

With these definitions in mind, we have analyzed most data loss prevention strategies and determined that the majority incorporate technological methods and use a "one size fits all" strategy as proposed by Taal et al. [1] But because no single mechanism prevents Data Leakage, we propose an additional model—truly, a strategy or set of considerations—that may help organizations reduce the risk of data loss. This set of factors should help Information Technology and Security stakeholders (1) better understand what data they hold; (2) better quantify the value of that data; (3) define what the loss of the organization's "crown jewels" would mean for the organization's business operations; (4) determine ancillary data loss consequences for the organization and its stakeholders; (5) balance loss mitigation steps against the organization's operations and efficiencies; and (6) understand that any modern strategy to reduce Data Leakage must be recursive. While a tall task, this set of considerations can be approached as an issue-spotting exercise, and we provide support for the model below.

2. Current Issues – Strategic Definitions for Addressing Data Loss and Leakage

In the very first instance, most (if not all) issues associated with data (and by extension, data leakage) incorporate a very basic issue: data growth has accelerated due to the varied means by which information can be generated or captured. [9] This modifies the DLP concern by volume and data type, especially since DLP is often an unintentional issue—the more data available, the greater the odds of an eventual problem, including data leakage issues.

The Cheap Storage Myth carries the same concerns, especially when combined with the multiplicity of data sources. [10] This does not argue that storage itself creates the issue. Instead, bandwidth and connectivity improvements that make the "just send it to me" an easy approach seem to multiply data by their very operation, which makes any single potential risk issue that comes from touches directly upon data multiply risk at the same rate. Again, more data may equal more potential data leakage.

Even if there is more data, knowing where the data resides may help mitigate attendant data leakage issues. Gaining this knowledge may be addressed, at least in part, through the traditional approach of generating a data map, which identifies, details, and documents the data owned and possessed by an organization. [11] But this may not be enough, as it can miss the dark and dusty data unknown to the present-day actors [12] as well as the data transfer mechanisms that operate as bit players, used only for a one-off data transfer or movement according to a fleeting purpose.

A more robust measure of defining data loss and leakage may therefore focus less on the "whole" and more on those areas where an approach will have the biggest impact on what actually matters for the organization. This approach has a number of benefits, not the least of which is avoiding the "boil the ocean" approach where every issue requires the same granularity.[13] The contrast, an iterative approach determining the best (e.g., most strategic) implementation steps [14], follows best practices within project management practice as well.[15]

Additional data loss mitigation strategies may take automated or "people-less" information governance approaches into consideration, where appropriate document classification and deletion and destruction steps will remove potential issues from a loss equation and limit an organization's risk footprint [16] or limit data storage geographies. [17] Appropriate and considered approaches will, of course, also incorporate employee behavior, general education, and directed training. [18]

3. Identifying Data States: Data in Use, Data in Motion, and Data at Rest

Data movement, stasis, and storage inform much of the DLP discussion and data leakage mitigation, even when considering additional factors. These issues comprise the verticals considered during traditional data loss analyses, and some commentators have proposed that certain solutions, such as the suite comprising information protection and control (IPC) measures (which include monitoring, encrypting, filtering, and blocking sensitive data), may be applied to all data within the organization whether in-use, in-motion, or at-rest. [19] However, we submit that DLP solutions offered to organizations are often limited in focus to one of the traditional use cases: endpoint data-in-use considerations; data center and endpoint data-at-rest issues; and enterprise network transverse movement issues associated with data-in-motion.[2] This may reflect honesty in the developers' or solution providers' appraisal of what any singular technology or solution can do and may even be supportive (if unemotionally) of the strategic iterative

approach we support above, but the use of just one singular solution may leave other issues unaddressed while giving a false sense of security to the purchaser. Instead, solutions should incorporate a multi-prong approach that incorporates both automatic [16] and personnel-driven approaches.[18]

Data in use. Data in use is the lifeblood of the organization, and the data that allows work to be performed. But data in use considerations also require a determination of storage system usage—such as file servers, databases, Microsoft SharePoint, and Documentum instances—and can help determine where connections currently exist, and where they should be strengthened, hardened, or, alternatively, severed.[20] An appreciation or understanding of what data in use means qualitatively must also note that if the data is unusable, it reverts to data at rest, not only losing its efficacy and purpose according to the organization's operations or design, but also implicating those considerations at play for the organization's *other* data at rest. Adding this and the below detail may therefore be critical for accurate data mapping efforts, as well as for determining what combination of solutions (technical as well as human, as discussed below) is appropriate given the organization's data footprint as well as its human capital issues.[18]

Data in motion. This movement of data considers the organization's connections, critically examining on a vertical, high-to-low-level analysis (and beginning at the macro level) of existing infrastructure and major implementations, such as electronic document management systems.[19] This examination also moves horizontally, extending out from the higher-level sources to encompass additional activities and related data movements across and within the organization's network. Such considerations include but are certainly not limited to: email, websites and web applications, Instant Messaging, File Transfer Protocol measures, cloud storage and applications, and other transfer and communication methods.[20][19]

While this examination is also critical for data mapping efforts, a change in status for this issue may convert data in motion to data at rest, intentionally or otherwise, and may implicate the organization's data at rest strategy. These are not idle considerations—the data does not exist in a steady state, and changes in data character as well as data use should be considered when developing organizational data strategy. Dynamism is the key, and these issues of time and change can change a two-dimensional analysis into a three- or four-dimensional set of considerations.

Data at rest. Data at rest, or the structured and unstructured data sources that may make up the vast majority of the organization's data footprint, therefore pose the largest (by volume) issue but may present the least technical challenge.[14] Typically, issues with data at rest focus and rely on encryption, with some tokenization and even air gaps included for good measure. But with the growing prevalence of mobile devices, even encryption issues have become more complex.[21] These issues include considering the differences between mobile hardware and software encryption.

Organizations may consider building these considerations into their BYOD policies[21] and further train their personnel to cover additional contingencies.[18] But organizations may need to also evaluate and consider additional user considerations through the pre-emptive use of DLP or other technologies in order to further identify sensitive data at rest and determine how to best handle or discard this data before users have the opportunity to interact with it.[19][16] This type of evaluation of data-at-rest may also incorporate a classification step, such as the traditional public-private-sensitive taxonomy.[19] These issues also factor into the data mapping process, and influence the strategy the organization undertakes in response to potential data leakage issues.[17]

4. The Defined Data Loss – Data Leakage, Damage, and Disappearance

Leakage. Even with a robust data map, an organization must also consider what a "data leakage" problem actually consists of. This step of analysis begins with considerations of and a straightforward reckoning as to whether data has leaked (or been leaked), has vanished, or been damaged beyond repair. Data Leakage includes, but is not limited to, those newsworthy instances where an intruder "is simply looking to harvest usernames and passwords, steal banking credentials or hijack computers for a botnet to send spam" through the use of spear-phishing, human intelligence [7], or waterhole attacks. [22] Here, data loss mitigation efforts should examine both the environment to determine what is technically feasible, but also examine the personnel surrounding the processes.[17]

Damage. Those instances where data may still exist but might be impossible to access [23] also constitute data loss instances, even if the organization opts to pay (and "lose") rather than retaliate or involve authorities—inaccessibility constitutes loss, especially when a ransom payment is the only way to access the data and support business continuity efforts.[24] Mitigation of loss can focus on training or mechanism to limit the negative effects associated with certain data interactions, but related backup procedures might be as (or more) effective in the long run for the organization, as seen and demonstrated in ransomware-type situations.[24]

Disappearance. Data does not need to end up in the possession of a third-party to constitute a loss, as data loss instances may also incorporate distributed denials of service (DDOS), malware infections, man-in-the-middle attacks, and ransomware infections that also qualify as losses.[17][24] This issue may also present where employees misplace data accidentally due to confusing information technology policies; shared drive or SharePoint policies that do not keep pace with internal change management processes; or simple, ineffective chain-of-custody practices. This may, as noted by

Sherer et al., include those instances where employees mean to—or in effect (while completely unintentionally)—delete or render data useless through the operation of information governance (IG) and its related practices when the purpose of those IG practices is instead to appropriately manage organizational data.[16] Again, back-ups may be an appropriate part of a multi-prong approach, where tapes are a disaster recovery mechanism but not the only solution to data disappearance prevention.[24]

5. Automatic Data Loss

Applied IG practices that create their intended effect, but where that effect is inappropriate given strategic organizational aims, are not employee or even person-dependent. These types of practices can include hardware or internal process failures, including cloud-specific computing outages or improper employee use.[22] They may also be situational in nature or event-driven—such as company mergers, acquisitions, asset purchases, or divestitures.[25]

These, in turn, can lead to data loss issues recognized by courts and regulators, such as the UBS purchase of Paine Webber in 2000 where the United States Securities and Exchange Commission (SEC) later alleged that UBS had failed to preserve former Paine Webber information related to its activities as a member of an exchange, broker, or dealer, and UBS agreed to penalties and fines to resolve these claims with the SEC, the New York Stock Exchange, and the National Association of Securities Dealers.[26]

When misunderstood or misapplied, the application of normal document and information deletion periods can sometimes inadvertently erase data that should have otherwise been saved. The task of cataloging and categorizing an organization's data may be a herculean undertaking and can lag behind actual practices even where the organization would be well served to create a data taxonomy or classification system.[4] These considerations factor into the four-dimensional model of data mapping, as semiautomatic factors that can be included as movement within the model, either as protections against data leakage (by automatic deletion) or mechanical steps that should be interrupted when subject to regulatory or legal hold issues.[25]

Solutions to this issue incorporate appropriate and considered document retention periods[16], as well as user and information technologist training.[18] Strategic approaches also note that expertise may be institutional in nature, a challenge especially present in deal-driven events such as mergers and acquisitions, where long-time employees (and their knowledge) exit the premises.[25] In those instances, debriefing of existing practices and implemented technology will assist in shutting off such automated practices that can, as designed, lead to automatic data loss incidents.

6. Data Loss According to Internal and External Stakeholders, Law or Regulation, and the Public at Large

Internal and external stakeholders. As noted elsewhere, a data breach or loss should not be considered as a single incident but as a series of related incidents.[27] What seems like a textbook incident of Data Leakage could turn out, *post mortem*, to be a feint within a feint, where the intruder both captures and alters data. These types of incidents and their changing characterizations highlight the issue as a whole, where the entire organizational team dealing with the incident must return, and return again, to evaluate the incident until the event is well understood, and the lessons have been learned. [28]

The majority of technical literature highlights the software and hardware failures and proposed solutions for post-incident detection, but this only represents half the issue, and perhaps the most integral part: the people. The people involved in incident prevention, response, and post-incident activities are the hearts and souls of both the problems and the responses. They comprise the least considered factor of current DLP strategies and the portion that deserves greater attention from security professionals—the human element. Certainly, the first line of incident response comes from the individuals responsible for assessing whether there has been a loss: the system administrators and technologists who have now recognized DLP among top budget priorities for several years [4] and who are primarily responsibility for detecting and preventing incidents. [7]

The story of the incident, however, does not end there. Those individuals who use the data and depend on its reliability [29] include those business people who are primary users of the data [5] but who may be unaware of how their uses of and access to that information can imperil it. [20] This demonstrates how critical training remains, as employees remain a critical part of mitigation strategies and recovery efforts.[18]

Law and Regulation. Data loss, as approached through the lens of legal and compliance regimes, may operate quite differently than a traditional set of considerations, even though the legal considerations are still considered direct losses.[30] In the instance of a data breach at a financial institution, a loss of personal credit information (PCI) may trigger reporting requirements, regardless of whether the PCI is actually "lost" or if the incident otherwise affects the operations of the enterprise.[27] This presents a challenge where, perhaps from information technology or operations perspectives, this does not qualify as data loss, disappearance, or even damage. In fact, the data in that instance is still present and operates exactly as it did before, but the scenario still fits the criteria of the other type of loss: Data Leakage. If the IT department is unaware of the organization's reporting requirements and fails to take required steps, any further evaluation of this particular incident might lead to harsher penalties, sanctions, and other ramifications.

In those instances, the evaluation by legal and compliance of the related regimes must also be part of that changing process. A decision made within twenty-four hours of an incident may be the right call for the organization at that point in time, but it must be revisited just as other conclusions about the incident are made. And security professionals, as well as those who rely upon them, must understand that an incident may not be resolvable even after a root cause analysis. As noted in one article, "If someone walks up to you on the street and hits you with a lead pipe, you know you were hit in the head with a lead pipe…[c]omputer security has none of that knowing you were hit in the head with a lead pipe."[7] These issues are further exacerbated when knowledgeable employees are not consulted regarding both their official roles and those tasks that are informally delegated or simply assumed. [25] This is an issue which is difficult (or impossible) to address by an automated mechanism; instead, tried-and-true communication strategies may lead to the best results for determining exactly how the organization's actual practices square with legal and regulatory requirements.[25][26]

The Public at Large. Further stakeholders include that set of subsequent users whose responsibilities are informed by the data's secondary effects (such as data analytics) to do the work of the organization. [5] This set is comprised of employees, contractors, and those individuals maintaining automated processes that take and use data feeds.[29] Finally, keeping within the organization, a number of additional parties are affected, directly or not, by data use and its potential loss. These include related components of an organization's internal operations, such as executive management, key business line executives, IT Security, compliance, human resources, and legal.[4]

Importantly, data loss that impacts individuals does not stop at the firewall. There are a number of diverse third-parties that may also be affected by data loss, which include (1) outside legal counsel for the organization as well as legal counsel for the organization's adversaries [31]; (2) other vendors (including cloud providers) who are tasked by the organization to assist with that data's protection; and (3) those customers, suppliers, and joint-venture partners who have entrusted the organization with their data and expect its availability, use, and protection.[27]

When considering each of the stakeholders, the enterprise must also consider the risks radiating from each, which may include (at least) "heavy fines, loss of customer confidence, loss of trade secrets, loss of competitive advantage, negative impact to brand, [and] customer attrition."[18] Unfortunately, even while the ramifications of loss are beginning to be better understood and recognized as one of the most critical enterprise issues [17] many of the potential solutions, or more accurately protections associated with data loss, are still evaluated according to economic benefit terms for the organization [32]—that is, some focus on one or a combination of "Return on Investment (ROI), Net Present Value (NPV) and Internal Rate of Return (IRR) as financial metrics for quantifying the cost and benefits of computer security expenditures." [33]

While we have thus far discussed legitimate users, we must also consider those legitimate insiders who engage in *illegitimate* use. Many access mechanisms, such as universal serial bus (USB) drives or bring your own device (BYOD) technologies [21], allow for work mobility but may be used to steal intellectual property. [34] Here, the best advice of "awareness within the organization and at home" is unavailing, as "nothing will stop a determined user from clicking a link or installing something" [22] once they have determined a path forward—especially when that path includes intentional deceit.

Career progression motivations for stealing information are not uncommon, for upwards mobility either within or outside the organization. These types of theft might involve many different data types: traditionally, "unstructured formulas, technical designs, source code, and manufacturing procedures."[18] But as proprietary "big data" sets grow and evolve in usefulness, these too—and related database reports—may occasion additional scrutiny.[35] These career progression motivations are not uncommon, and most such attacks are conducted directly for financial gain.[31]

But not every related attack considers financial gain, and there is now a tradition of users who affect the data for some combination of profit, politics (such as the WikiLeaks-related disclosures) [20], or fun (the "4chan-type" hackers or "script kiddies") while sometimes simultaneously gaining data as a proxy for identity theft or subsequent sale.[36] Unsurprisingly given the description, practitioners must remember there is no guarantee that such attacks will be extraordinarily complicated or insightful, as Richardson reported that most data breaches "required no or only a low degree of skill to perpetrate" [33], and PWC stated that the cybersecurity programs of most organizations "do not rival the persistence, tactical skills, and technological prowess of their potential cyber adversaries."[31]

7. Returning to the Individual

Personal considerations as how to use data are exactly that: decisions made according to personal decisions each time data is utilized away from scripted circumstances (such as the operation of automatic programs). Because these user interactions are not scripted, a focus on average or normal individual behaviors and associated training may be the most important single decision given a specific technology.[18] The extent to which most incidents are caused directly or indirectly by user error is large enough that time invested in endpoint interactions may be most efficiently spent when considering the technologies the employees actually use: laptops, desktops, smart phones, removable media, BYOD, and transfer mechanisms to a non-enterprise-supported cloud.[20] Training is not, however, likely to be entirely sufficient. Additional interviews and related deep-dive determinations of actual employee and related individual

practices can offer the best view into what is happening in an organization. Unfortunately, these require time, attention, and expenditure, which might be available only at times of scrutiny [21] or transition—and sometimes not even then.[25]

This focus on the individual can also help discern the organization's trajectory, and can assist the organization and its security professionals in determining where future efforts are best spent. This practice of monitoring employee behavior serves two goals: (1) it assists with DLP efforts generally; and (2) it helps determine where the organization is going as an entity, better positioning security (and other) professionals to develop practices and incorporating technologies to address future activities in a practical and realistic matter. There are additional considerations for these types of monitoring programs, however, including data privacy and governance issues.[37] But companies can address these types of issues successfully when allowing employees additional freedoms to work in the way most appropriate to their needs, while still protecting organizational assets and casting a broad net of protection.[21]

8. Conclusions

The approach we consider in this article is part script, part improvisation, which begins with a robust data map but quickly pushes it into four-dimensions while keeping a close eye on the employee element without being overly directive. This approach should provide flexibility and balance, giving the employees the opportunity to do their jobs to the best of their ability without giving them either too much restriction or sufficient rope to hang themselves.

We suggest that a balancing test might be most appropriate for the majority of these issues, as not every data loss issue will be categorized at the same level and not every data instance will be amenable to all of these solutions. And just because the application of a particular solution is possible, it may not be practical (*e.g.*, to make every login 300 characters) given the organization's aims and need to do business. Rather, we submit that a more measured evaluation and considered approach is the best route forward, especially as we submit that there truly is no one-size-fits-all or one-approach-solves-all problems exists.

Acknowledgements

We are very grateful to Kelly Singleton, Emily Fedeles, and Nichole Sterling for their assistance in support of this article.

Disclaimer

The views expressed herein are solely those of the authors, should not be attributed to their places of employment, colleagues, or clients, and do not constitute solicitation or the provision of legal or security advice.

REFERENCES

[1] Taal A, Jenson KS, Sherer JA, Ponce de Leon A & Le J. How a Nuanced Approach to Organizational Loss may Lead to Improved Policies, Better Applied Technologies, and Greater Outcomes. International Conference on Cyber Warfare and Security, Academic Conferences International Limited; 2016.

[2] Elastica. The 7 Deadly Sins of Traditional Data Loss Prevention (DLP) in the New World of Shadow IT [Internet]. White Paper; 2014. Available from: https://www.elastica.net/ebook-7sins-dlp/.

[3] Kanagasingham P. Data Loss Prevention [Internet]. SANS Institute InfoSec Reading Room; 2008. Available from: https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883.

[4] ISACA. Data Leak Prevention [Internet]. White Paper; 2010. Availablefrom:http://www.isaca.org/Groups/Professional-English/security-trend/GroupDocuments/DLP-WP-14Sept2010-Research.pdf.

[5] Liu S & Kuhn R. Data Loss Prevention [Internet]. IT Pro; 2010.Availablefrom:http://csrc.nist.gov/groups/SNS/rbac/documents/data-loss.pdf.

[6] Dart E, Rotman L, Zurawski J, Hester M & Tierney B. The Science DMZ: A Network Design Pattern for Data-Intensive Science. Scientific Programming, Vol. 22, Issue 2; 2014.

[7] Zetter K. Everyone Has Been Hacked. Now What? [Internet]. WIRED Security; 2012. Available from: http://www.wired.com/2012/05/everyone-hacked/.

[8] Greenberg P. Security Breach Notification Laws [Internet]. National Conference of State Legislatures (NCSL); 2015. Available from: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[9] Chang V & Ramachandran M. Towards Achieving Data Security with the Cloud Computing Adoption Framework. IEEE Transactions on Services Computing, Vol. 9, Issue 1; 2016.

[10] Knight J & Cumming K. Digital Data Hoarding and the Implications for RIM Professionals. IQ: The RIM Quarterly, Vol. 28, Issue 3; 2012.

[11] Isaza JJ. 10 Things Organizations Should Do to Protect Against Hacking. Information Management, Vol. 48, Issue 5; 2014.

[12] Iven J & Lamanna M. Overview of LHC Storage Operations at CERN: CERN IT File-based Physics Data Storage Operations in 2011/2012. Journal of Physics: Conference Series, IOP Publishing, Vol. 396, No. 4; 2012.

[13] Shaw C & Hamilton R. Customer Experience is a Journey, Not a Destination. The Intuitive Customer, Palgrave Macmillan UK; 2016.

[14] Rogowski W. The Right Approach to Data Loss Prevention. Computer Fraud & Security, No. 8; 2013.

[15] SanAgustin AJ. Case Studies in Managing Change. Information Management, Vol. 48, No. 4; 2014.

[16] Sherer JA, Selby J & Rovine J. Opting for a New Approach to Information Governance – Simple Principles with Outsized Effects [Internet]. Bloomberg BNA Digital Discovery & e-Evidence, 14 DDEE 482; 2014. Available from: https://www.bakerlaw.com/files/uploads/Documents/News/Articles/LITIGATION/2014/10-9-2014-Sherer-Selby-Rovine-Bloomberg-BNA-Digital-Discovery-e-Evidence.pdf.

[17] Kale AV, Dubey SP & Bajpayee V. A Review on Data Leakage Prevention. International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 4, No. 4; 2015. Available from:http://ijcsmc.com/docs/papers/April2015/V4I4201599a23.pdf.

[18] Symantec. Guide to Successful Data Loss Prevention Risk Reduction [Internet]. White Paper; 2013. Available from: https://www.intelisecure.com/wp/wp-content/uploads/2014/10/Guide-to-Successful-Data-Loss-Prevention-Risk-Reduction-Part-1.pdf.

[19] Nawafleh SA, Hasan MYF, Nawafleh Y & Fakhouri SAR. Protection and Defense against Sensitive Data Leakage Problem within Organizations [Internet].European Journal of Business and Management, Vol. 5, No. 23; 2013. Available from: http://www.iiste.org/Journals/index.php/EJBM/article/view/7478/780.

[20] McAfee. Combating the Insider Risk to Data [Internet]. White Paper; 2010. Available from: http://www.mcafee.com/us/resources/solution-briefs/sb-combating-insider-risk-to-data.pdf.

[21] McLellan M, Sherer J & Fedeles E. Wherever You Go, There You Are (With Your Mobile Device) [Internet]. 21 RICH. J.L. & TECH. 11; 2015. Available from: http://jolt.richmond.edu/index.php/wherever-you-go-there-you-are-with-your-mobile-device-privacy-risks-and-legal-complexities-associated-with-international-bring-your-own-device-programs/.

[22] Turner M. How to Prevent Employees from Compromising your Data [Internet]. InfoSecurity Magazine; 2015. Available from: http://www.infosecurity-magazine.com/opinions/prevent-employees-compromising-data/.

[23] Donaldson S, Siegel SG, Williams C K & Aslam A. Defining the Cybersecurity Challenge [Internet]. Enterprise Cybersecurity, Apress; 2015. Available from: http://link.springer.com/chapter/10.1007%2F978-1-4302-6083-7_1.

[24] Ragan S. Ransomware Isn't a Serious Threat Says Threat Intelligence Firm [Internet]. CSO Online; 2015. Available from:http://www.csoonline.com/article/2879697/data-protection/ransomware-isnt-a-serious-threat-says-threat-intelligence-firm.html.

[25] Sherer JA, Hoffman T & Ortiz E. Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, E-Discovery, and Information Governance into Due Diligence Practices [Internet]. 21 RICH. J.L. & TECH. 5; 2015. Available from: http://jolt.richmond.edu/index.php/merger-and-acquisition-due-diligence-a-proposed-framework-to-incorporate-data-privacy-information-security-e-discovery-and-information-governance-into-due-diligence-practices/.

[26] Securities and Exchange Commission (SEC). Order Instituting Administrative and Cease-And-Desist Proceedings, Making Findings, and Imposing Remedial Sanctions and a Cease-And-Desist Order Pursuant to Section 15(b) and Section 21C of the Securities Exchange Act of 1934 [Internet]. Release No. 52022; 2005. Available from: https://www.sec.gov/litigation/admin/34-52022.pdf.

[27] Guffin P. Data Security Breach Notification Requirements in the United States: WHAT YOU NEED TO KNOW [Internet]. InFocus Magazine; 2011. Available from: http://www.pierceatwood.com/webfiles/Data%20Security%20Breach%20Notification%20Requirements%20in%20the%20United%20States%20by%20Peter%20Guffin%20(W2853836).PDF.

[28] Stone-Gross B. Malware Analysis of the Lurk Downloader [Internet] Dell; 2014. Available from: http://www.secureworks.com/cyber-threat-intelligence/threats/malware-analysis-of-the-lurk-downloader/.

[29] Harvard Business Review (Harvard). The Evolution of Decision Making: How Leading Organizations Are Adopting a Data-Driven Culture [Internet]. Harvard Business Review Analytic Services; 2012. Available from: https://hbr.org/resources/pdfs/tools/17568_HBR_SAS%20Report_webview.pdf.

[30] Shabtai A, Elovici Y & Rokach L. A Survey of Data Leakage Detection and Prevention Solutions [Internet]. SpringerBriefs in Computer Science; 2012. Available from: http://www.springer.com/us/book/978146142.

[31] PricewaterhouseCoopers (PWC). US Cybercrime: Rising Risks, Reduced Readiness [Internet]. White Paper; 2013. Available from:http://www.globalinitiative.net/wpfb-file/pwc-us-cybercrime-rising-risks-reduced-readiness-key-findings-from-the-2014-us-state-of-cybercrime-survey-june-2014-pdf/.

[32] Geer DE Jr. Security of Information When Economics Matters [Internet]. Verdasys White Paper; 2004. Available from: http://craigchamberlain.com/library/insider/Economic_files/Security%20of%20information%20When%20Economics%20Matters.pdf.

[33] Richardson R. CSI Computer Crime and Security Survey [Internet]. Computer Security Institute; 2008. Available from: http://www.kwell.net/doc/FBI2008.pdf.

[34] Silowash GJ & King C. Insider Threat Control: Understanding Data Loss Prevention (DLP) and Detection by Correlating Events from Multiple Sources [Internet]. Carnegie Mellon Software Engineering Institute Technical Note CMU/SEI-2013-TN-002; 2013.

[35] Olhorst F. Big Data Analytics: Turning Big Data into Big Money. John Wiley & Sons, Inc.; 2013.

[36] Stryker C. Epic Win for Anonymous – An Online Army Conquers the Media. The Overlook Press; 2011.

[37] Kim J & Hyung JK. Design of Internal Information Leakage Detection System Considering the Privacy Violation. 2010 International Conference on Information and Communication Technology Convergence (ICTC); 2010.