IEEE Access
The journal for rapid open access publishing

Received October 31, 2015, accepted November 29, 2015, date of publication December 7, 2015,
date of current version December 16, 2015.

Digital Object Identifier 10.1109/ACCESS.2015.2506185

Data and Information Leakage Prevention Within the Scope of Information Security

BARBARA HAUER
Johannes Kepler University Linz, Linz 4040, Austria
Corresponding author: B. Hauer (barbara_hauer@gmx.at)

ABSTRACT Incidents involving data breaches are ever-present in the media since several years. In order to overcome this threat, organizations apply enterprise content-aware data leakage prevention (DLP) solutions to monitor and control data access and usage. However, this paper argues that current solutions are not able to reliably protect information assets. The analyses of data breaches reported in 2014 reveal a significant number of data leakage incidents that are not within the focus of the DLP solutions. Furthermore, these analyses indicate that the classification of the provided data breach records is not qualified for detailed investigations. Therefore, advanced criteria for characterizing data leakage incidents are introduced, and the reported records are extended. The resulting analyses illustrate that DLP and information leakage prevention (ILP) demand various information security (IS) measures to be established in order to reduce the risk of technologically based data breaches. Furthermore, the effectiveness of DLP and information leakage prevention (ILP) measures is significantly influenced by non-technological aspects, such as the human factor. Therefore, this paper presents a concept for establishing DLP and ILP within the scope of IS.

INDEX TERMS Security, information security, data security, information leakage prevention, data leakage prevention, information exposure.

I. INTRODUCTION

A. MOTIVATION

This article focuses on data leakage prevention (DLP) and information leakage prevention (ILP) within the scope of information security (IS) which exceeds information technology (IT) security. The terms DLP and ILP are not accurately specified in any official standard or regulation. Hence, a lot of terms and definitions are applied in the context of DLP which gives rise to confusion and misapplication. Vendors use the term DLP to advertise products which offer full or single DLP capabilities as an out of the box solution for solving information exposure issues. However, they are vague about specific DLP functionalities and the relevance of these features. Therefore, Section I-B of this work addresses DLP and ILP in general, the basic concepts of DLP, used data classification techniques including their blind-spots, as well as the challenge to detect data.

In order to gain knowledge about recent data leakage incidents, Section II presents a survey of data breaches reported in 2014. Due to the fact that the classification of the provided data is not qualified for detailed analyses, this work proposes advanced criteria for characterizing data leakage incidents as well as certain criteria for characterizing the relevance of attacks in Section III and Section IV, accordingly.

The analysis of data leakage incidents based on these advanced criteria illustrate that DLP and ILP demand measures to be implemented in various IS areas. Furthermore, DLP and ILP involve technological and non-technological aspects which do not allow pure IT-based approaches. Hence, the human factor becomes important. On the one hand, it is essential to identify data, information, and knowledge worth protection, to figure out where those are located in which form, to appraise their intangible assets, and to correctly estimate all sorts of relevant risks. On the other hand, organizations rely on the acceptance and the cooperation of their employees because there is no never-known-to-fail method to prevent leakage. Therefore, Section V of this work introduces a coherent concept consisting of various elements for establishing DLP and ILP within the scope of IS.

B. STATE OF THE ART DLP SOLUTIONS

This article refers to DLP as data leakage prevention and ILP as information leakage prevention whereas commonly used synonyms [1] such as data loss prevention (DLP), extrusion prevention (EP), content monitoring and filtering (CMF), content monitoring and protection (CMP), information leak prevention and detection (IDLP), outbound content

compliance (OCC), or information protection and control (IPC) are not described in detail.

State of the art DLP solutions, also referred to as enterprise content-aware DLP solutions, offer different approaches to monitor and to protect confidential data at client endpoints. A survey of market leader products can be found in [2]. Typically, these solutions validate and authorize applications before allowing confidential data to be transferred and to be migrated. Furthermore, data usage on client endpoints and network traffic are monitored, and copy and paste operations and taking screenshots can be prevented. In general, current DLP solutions are able to control the access to confidential data and the utilization of this data by the user. Moreover, the systems can prevent unauthorized users or applications to obtain confidential data. But there are several issues and limitations.

Basically, the ISO/IEC 2382 standard specifies data as a ''representation of information in a formalized manner, which should be suitable for communication, interpretation, or processing'' [3]. Based on Norths stairs of knowledge definition, data consists of characters which are connected by syntax. A sequence of characters, such as a numerical value, only becomes information if its meaning is known, e.g. the numerical value is an amount. A correct combination of information imparts knowledge, e.g. the amount belongs to the highest bidder. This knowledge can lead to an appropriate activity [4]. In general, preprocessed information or concrete knowledge is provided to the user. Therefore, information exposure is ''the intentional or unintentional disclosure of information to an actor that is not explicitly authorized to have access to that information'' [5].

Due to the fact that DLP focuses on data, this technique provides insufficient means to reduce the information exposure risk which can be seen as part of ILP. Further challenges of DLP refer to possible weaknesses in the scalable rights management, the proper access control, and the monitoring. The complexity involved in these fields of IS gives rise to potential failures. For example, a strict access control is ineffective if every employee of an organization has access to all systems and data within the IT infrastructure. Another example is sharing user accounts on various systems which is frequently applied to administrator and root accounts.

1) STATES AND CLASSIFICATION OF DATA

A reasonable classification of data is an integral component of DLP since it has a major impact on the proper handling of data and hence the applied security requirements. For example, data classified as top secret is subject to other restrictions in handling than data classified as restricted or public.

Furthermore, the handling of data depends on whether data is present as

- data in use (DIU),
- data at rest (DAR), or
- data in motion (DIM).

Unfortunately, the classification of data results is a major challenge since organizations are frequently confronted with a large amount of data which prevents manual classification. Moreover, they avoid to trust employees implicitly and the classification level may change during data lifetime. As long ago as 1961 an article entitled ''Automatic Indexing: An Experimental Inquiry'' was published which proposed a ''technique for automatically classifying (indexing) documents according to their subject content'' [6]. Since then indexing has been advanced to classification using key words, dictionary search, regular expressions, and even machine learning techniques. Accordingly, DLP classification techniques overlap with data mining and knowledge discovery in databases (KDD) techniques.

In 2013, Gartner, Inc. published a report on ''Enterprise content-aware DLP'' [7]. Compared to the Forrester Wave report published in 2008 [8], the leadership in the market has been slightly shifted due to various buyouts. Companies, which offer products and solutions with DLP functionalities for DIU, DAR, and DIM, are referred to as market leaders. Their holistic approach stands in contrast with channel DLP and DLP-lite solutions which are limited to single capabilities like DLP for e-mail, web, or removable media. In order to be efficient, DLP solutions have to pay attention to mobile devices and their increasing relevance in business applications as well. In case of addressing mobile data protection (MDP), the leadership in the market for enterprise content-aware DLP solutions can be reduced to McAfee [9], Symantec [10], Digital Guardian formerly known as Verdasys [11], and Websense [12].

In consideration of product data sheets, white papers, and administration guidelines published by the market leaders, the products provide improved DLP capabilities, especially classification techniques, compared to 2008. The market leaders seem to attempt compliance with regulations and standards such as

- the Payment Card Industry Data Security Standard (PCI DSS),
- the Health Insurance Portability and Accountability Act (HIPAA),
- the Federal Information Security Management Act (FISMA),
- the Gramm-Leach-Bliley Act (GBLA), and
- the Control Objectives for Information and Related Technology (COBIT).

These regulations and standards are demanded by several and frequently financially strong customers. Unfortunately, this compliance only requires fundamental DLP classification techniques such as searching for key words and regular expressions. This can lead to a high false positive rate (FPR), particularly when classifying unstructured data. For example, a regular expression search assumes that credit card numbers provide a consistent format with minor deviation referring to, for example, spaces and hyphen. Key word searching typically relies on key words common for a specific sector of industry. This can negatively affect the detection rate since not all synonyms, translations, dialect words, misspellings, and abbreviations of a key word are considered.

Content-awareness influences the detection rate and thus the classification because one word can have different meanings or a different correlation to a person. Context-aware, content-aware, and/or behavioral analyses are used in combination with

- key words and regular expressions,
- digital fingerprints,
- data tagging, and
- machine learning techniques

for classifying sensitive data. In addition to key words and regular expressions, digital fingerprints are commonly used for digital signatures and for searching text fragments. In this context, the size of the chosen text fragments is of high relevance. On the one hand, choosing too big fragments may result in a low detection rate. On the other hand, choosing too small fragments may increase the FPR. The fingerprint technique is used for plagiarism detection, too. In both applications, DLP and plagiarism detection, the fingerprint technique is facing issues with translations and text in pictures. In general, basic DLP solutions still make use of key words, in some cases extended by regular expressions and digital fingerprints. Several vendors utilize data tagging which can positively affect the handling of large data volumes if the tags can be considered trustworthy. These tags have to be chosen by the data creator or the DLP solution.

Various market leaders and visionary vendors additionally implemented findings of academic research. Some of these advanced solutions rely on machine learning techniques such as a support vector machine (SVM) which allows to handle large quantities of data. These techniques are well known in the field of data mining, KDD, spam filtering, face detection, and long term weather forecasts. However, in order to gain an acceptable recognition rate it is important to provide a good training data set containing a sufficient number of positive and negative examples for learning. This can be quite challenging. Results, which were published in 2011, show that a naive approach for training a classifier will lead to a high FPR [13]. These results are based on evaluated algorithms for text classification on confidential documents which are written in English and published on WikiLeaks and other archives. Encrypted documents or documents containing multimedia content are not considered.

The study in [14] declares the follow statement: ''State of the art technologies for DLP aim to discover sensitive information in data, e.g. for regulatory compliances such as HIPAA 1 and PCI-DSS 2, but do not have any automated mechanisms to measure the value or sensitivity of individual data items. For instance, these systems treat a file with a credit card number and a file with 100 credit card numbers equally.'' As a consequence, this statement can be identified as a justification for advanced content-aware and context-aware DLP rules. A file with hundred credit card numbers processed by an employee of a financial institute or tested by a financial software can be quite usual. But in case of being transferred unencrypted or being accessed by a software engineer, an alarm should be activated. In addition, arrangements for authentication, authorization, access control, and allowed encryption should be considered as well as business processes.

In general, automated data classification as well as automated re-classification are techniques to handle large amounts of data. Especially automated re-classification can assist in preventing unintentional disclosure but even market leaders do not or do not fully support this feature.

2) DETECTION OF DATA

The presented techniques for automated data classification commonly have to detect data and to recognize the content in order to classify it. All market leaders show detection weaknesses when it comes to unstructured data, cloud support, non-English languages, unsupported data formats, multimedia data, or operating systems other than Microsoft Windows or Apple Macintosh Operating System (Mac). Therefore, methods for automatic content identification and data tagging are interesting applications for DLP, too. Techniques based on watermarking or robust hashes can enhance the chances of detection and identification. Various sophisticated DLP solutions try to introduce behavioral analytics but these efforts are in the early stages. Nevertheless, the issue of detecting and identifying data is a major challenge. Due to the existence of encryption, hidden channels, unsupported data formats, as well as a large amounts of multimedia data, DLP solutions can only work within limits.

3) SEPARATION OF DATA

Several DLP client agents, mobile agents in the context of mobile device management (MDM), and bring-your-own-device (BYOD) solutions provide two separated systems in sandboxes. Frequently, these sandboxes are also called containers. Each system in a sandbox has its own operating system, applications, policies, and data. Typically, one system contains business data and is therefore controlled by the IT department of the organization. The second system remains private for individual use of the owner. A further approach is based on a single system which includes the operating system and installed applications. In this context, the sandboxes are related to selected applications. These containerized applications are used to allow a separation between business and private applications and data. Both approaches can deny access and wipe data, systems, or even the device by remote control. In essence, the approaches try to create a protected environment which has full control over the contained data and the usage of the data.

II. SURVEY OF DATA AND INFORMATION LEAKAGE INCIDENTS

In the context of DLP and ILP, there is a wide range of threads which lead to data and information leakage incidents. In order to enhance security mechanisms and to prevent data leakage as effectively as possible, the major objective is to analyze and understand past incidents and attacks.

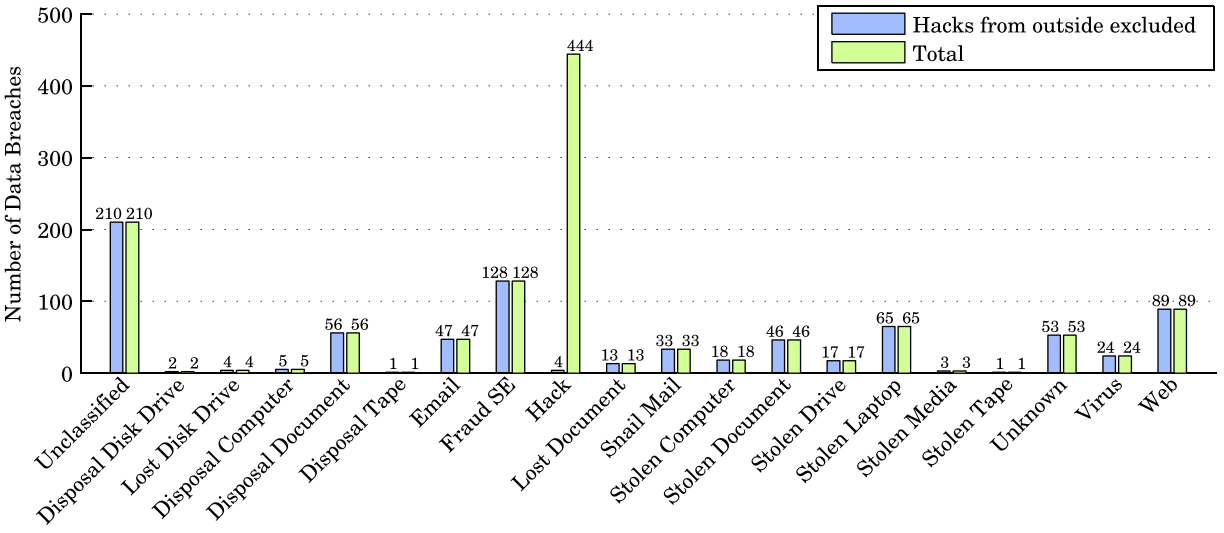

FIGURE 1. Distribution of data breach types reported in 2014.

This work makes use of a database called Datalossdb [15] which contains information about data breaches of personally identifiable information (PPI) reported by members of the Open Security Foundation. This information is requested from certain state governments which have enforced a Freedom of Information or Open Records legislation, a Breach Notification legislation, and a centralized authority for notification. In the United States of America (USA) only twelve states meet all these requirements, 35 states have enforced a data loss notification legislation without centralized reporting, and four states do not demand data loss notification at all. In Europe the European Cybercrime Centre (EC3), which is supposed to develop a common standard for uniform cybercrime reporting and to alert member states authorities, was launched in January 2013. Yet, only operators of critical infrastructure and public administrations are required to report serious network and information security (NIS) incidents to the national competent authorities. Furthermore, there is no official statement whether cybercrime related information has to be released to the public. This limitation prevents the acquisition and analysis of leakage incidents by the public and as a consequence, the enhancement of DLP and ILP related security measures is constrained.

The analysis presented in this work is based on 1259 data breaches of PPI reported in 2014. These records are confined to incidents fitting the criteria specified by the Open Security Foundation which do not include so called fringe incidents in favor of a consistent data set. Furthermore, the data is adjusted and double entries are removed. The interpretation of the data is conducted on the assumption that the number of unreported and undetected cases is significant due to the lack of a reporting obligation and a high number of imperfect data sets. But it is also assumed that the reported data breaches are able to exemplify leakage incidents in general.

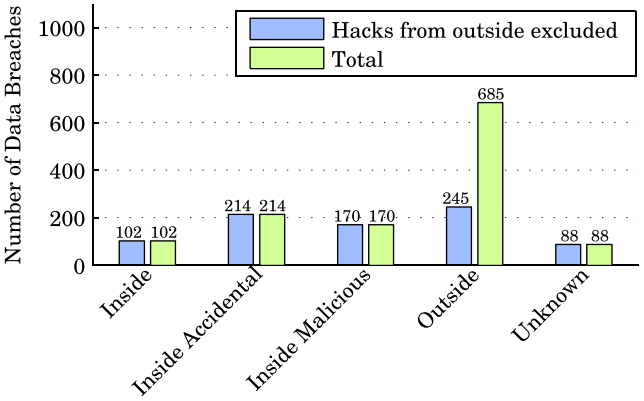

FIGURE 2. Distribution of data breach sources reported in 2014.

Basically, each record extracted from the database contains dedicated fields for the data breach type, the source of the data breach, the affected data types, certain dates of the data breach, and the textual description. The diagrams in Figure 1, Figure 2, and Figure 3 demonstrate the distribution of data breach types, data breach sources, and affected data types, accordingly. In this context, the term unknown is used to represent data which is not available. Due to the fact that this work focuses on DLP and ILP, hacks from outside are not of further interest because these incidents are mainly related to other aspects of IS. Therefore, the number of data sets not containing the key words ''hack'' and ''outside'' in the appropriate fields are shown separately. For example, the data type intellectual property was involved in three data breaches which were all caused by hacks from outside.

Figure 1 shows that hack as a data breach type was reported most often, closely followed by unclassified which sums up to 263 incidents with the data breach type unknown. This is equivalent to approx. 20 % in total and to over 30 % in case of excluding hacks from outside. As a consequence, a notable

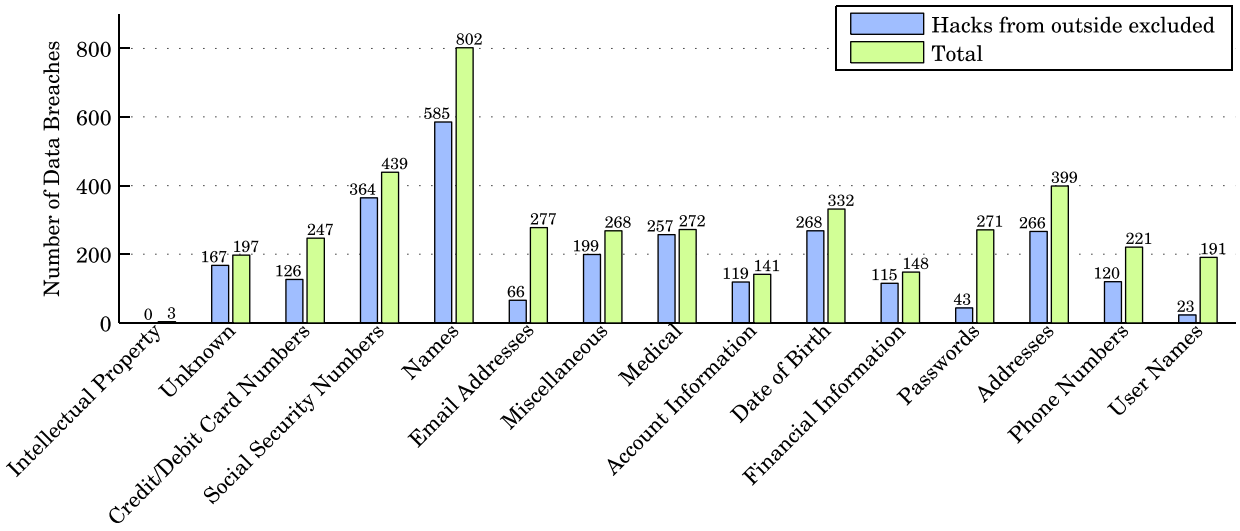

FIGURE 3. Distribution of data types affected by data breaches reported in 2014.

percentage of data breaches cannot be assigned to a specific data breach type without inspecting the textual description which can lead to further insights. A large number of fraud, scam, and social engineering incidents can be associated with a source inside an organization. However, insiders usually leak data unintentionally, for example, by careless publication on the web, incorrect usage of e-mails, and inappropriate handling of corporate documents and devices, in particular mobile devices.

Figure 2 illustrates that approx. 50 % of all data breaches are associated with the data breach source outside. In case of excluding hacks from outside, this number drops and the percentage of cases, in which insiders are involved, increases from approx. 40 % to almost 60 %. The high ratio of insiders marks the significance of considering the employee in DLP and ILP measures for organizations.

The distribution of data types affected by data breaches, which is demonstrated in Figure 3, indicates that the protection of names, social security numbers, addresses, dates of birth, and medical data should be emphasized. Especially names and social security numbers seem to be most frequently affected by data breaches. E-mail addresses, user names, and passwords are considerably more vulnerable by hacks from outside than by other data breach types and sources. The records of affected addresses, credit/debit card numbers, and phone numbers show a similar but less marked tendency. The number of incidents associated with the data type medical and unknown is almost not affected by hacks from outside.

III. ADVANCED CRITERIA FOR CHARACTERIZING DATA LEAKAGE INCIDENTS

A. CONCEPT AND TERMINOLOGY OF ADVANCED CRITERIA

These days available IS measures and IT security solutions are not able to prevent leakage incidents without exception. Of course, it is possible to reduce the probability of incidents but there is a remaining risk which cannot be eliminated. However, past incidents, which exposed information and leaked data, can be used to detect security deficiencies, to implement preventative measures, and to estimate remaining risks. For these purposes it is necessary to simplify the analysis of data breaches records. Therefore, this work proposes an extension of data breach records by advanced criteria which are listed in Table 1 and detailed in the following sections.

The proposed criteria are able to describe incidents at a certain level of abstraction which allows efficient analyses. The correct interpretation and accurate disclosure of incidents offer a precise definition of deficiencies. Moreover, clearly defined leakage incident records increase the traceability and avoid misinterpretation.

1) PARTICIPANT(s)

Incidents related to information exposure and data leakage are not necessarily caused by insiders. Several incidents, e.g. industrial espionage, malware, retributive action, and hardware lost in repair, can involve external persons. In case of outsourcing, employees of trusted business partners (TBPs) might have access to sensitive data, too. Furthermore, there are incidents with multiple participants sharing knowledge, privileges, and possibilities to cover traces.

2) INTENTION

In the majority of cases it can be assumed that a person, who applies for a job or is satisfied with a job, is not malicious. Hence, unintended data breaches are more likely than intended ones. Examples for such unintended incidents are forwarded e-mails containing internal information, sensitive data printed on envelopes, e-mails sent to outdated addresses, or failures due to software updates. Nevertheless, employees can be blackmailed to steal documents or might not be able

TABLE 1. Advanced criteria for characterizing data leakage incidents.

Participant(s) Internal, TBP, External
Intention Intentional, Unintentional
Access Point Inside, Outside
Access Mode Technological, Non-technological
Identity Correct, Shared, Stolen
Privilege Authorized, Non-authorized
Data Classification Top Secret, Secret, Confidential, Restricted, Unclassified (as defined by the organization)
Data State DIM, DIU, DAR
Information Value Knowledge, Information, Data
Communication Channel Permitted and Monitored, Permitted, Forbidden
Communication Medium Storage Medium, Endpoint Device, Network
Communication Mode Visible, Hidden, Encrypted
Incident Detection Internal Automated, Internal Manual, External Automated, External Manual, Other
Recurrence Risk Critical, High, Medium, Low, Medium

to resist the temptation if an organization does not adequately protect valuable information.

3) ACCESS POINT

The starting point of an attempted data access is not necessarily located within the business premises of an organization. External attackers usually try to grant access to the IT infrastructure of an organization from external locations by, for example, infiltration of malware. Furthermore, data leakage can also take place at TBPs and authorities. Common threats are stolen hardware, sold test hard drives, hacked servers, specific malware, software snooping around, and malicious employees. Furthermore, state of the art technology allows employees to work out of the office in almost the same manner as within the business premises of an organization. For example, a virtual private network (VPN) is commonly used on portable devices for remote access and smartphones are used to check e-mails. These devices can easily be stolen or lost. Conversations out of the office, e.g. in public means of transport, can be overheard. If possible, data classified as top secret should always stay within the business premises because security solutions are most qualified and effective at this location.

4) ACCESS MODE

Technological systems, such as IT systems, usually provide certain external interfaces which can be defended and controlled by available means. Non-technological threats, e.g. conversations in the public and handwritten notes, do not offer those interfaces. Hence, only training of awareness is able to protect from non-technological threats.

5) IDENTITY

In case of effective IT security measures, a suspicious log entry can easily be assigned to a unique user account of the organization. However, various organizations allow their employees to share highly privileged accounts for administration or for testing and as a consequence, assigning an incident to a specific person is almost impossible. Moreover, it is generally difficult to associate a user account with a person's identity because the person could be a victim of an attack, the user account could be stolen, or it could be unintentionally shared.

6) PRIVILEGE

DLP measures are meaningless in case of missing access control in the local area network (LAN), document accessibility without authorization, or highly privileged accounts for every user. It is a common problem that access rights are not updated, user accounts of former employees are not disabled in a timely manner, and user accounts are reused including the inherited rights. Therefore, a reasoned rights and access management, e.g. based on the Need-To-Know principle, and a role based access control (RBAC) are essential to comply with regulations and standards, and to provide the basis for DLP.

7) DATA CLASSIFICATION

The classification of data with respect to data breaches is important since incidents related to a certain classification, e.g. restricted, may occur more frequently than others. This could be an indicator that the protection of the data class is not efficient or that data is misclassified repeatedly.

8) DATA STATE

In general, DLP solutions differentiate between DIM, DIU, and DAR. If an e-mail was intercepted during transmission, the data was in the DIM state while being stolen. In cases of sensitive documents being stolen from a public network share, the accessed data was in the DAR state. Copying internal documents from a client endpoint to a private USB device as well as taking a screenshot of sensitive data are subject to DIU.

9) INFORMATION VALUE

In information science there are different concepts, models, definitions, and ideas associated with data, information, and knowledge. As mentioned in Section I-B, this work examines data and information from a non-technological and a technological point of view. A widely recognized non-technological model in information science and knowledge management is the data-information-knowledge (DIK) hierarchy [16]. The DIK model and most of its enhanced variations, such as

Norths stairs of knowledge [4], consider data as the basis of the hierarchy. Data given in a context becomes information and information given a meaning becomes knowledge. From a technological perspective, data represents information in a formalized manner [3]. Hence, knowledge has to be decompiled into information and information has to be decompiled into data since technology can only handle and store data.

Incomplete raw data sequences without known meaning are not as valuable and desirable as data which contains specific information. Therefore, the protection has to be adapted under consideration of the information value as well as the data classification. In the majority of cases it is not possible to protect data and information equally due to the large amount of data.

10) COMMUNICATION CHANNEL

Malicious usage of communication channels involve, for example, the improper handling of folders with patient letters, the transfer of data to private USB devices, and the usage of covert channels. In this context, the identification of covert channels is a major challenge. However, their usage requires certain qualifications, e.g. technical knowledge and adequate user privileges. In general, permitted communication channels, such as e-mail, web, and telephone, are commonly affected by data leakage and information exposure due to missing or weak monitoring.

11) COMMUNICATION MEDIUM

The communication medium is a determining criterion for preventing future data leakage. Incidents caused by stolen laptops can be prevented by, for example, using encryption, pre-boot authentication, and strong authentication solutions. If incidents frequently involve the network infrastructure, increasing the network security and monitoring have to be considered. In general, the involved communication medium is able to identify missing security mechanisms.

12) COMMUNICATION MODE

The communication mode refers to the effectiveness of monitoring as well as to the user privileges. State of the art DLP solutions are able to detect sensitive documents transferred in e-mails as well as not supported encryption. There are plenty of tools which can be installed on IT systems and misused to encrypt and hide data. However, their installation and usage should be prevented by correctly assigned user privileges or detected by endpoint surveillance.

13) INCIDENT DETECTION

The source of the detection indicates the strengths and weaknesses of certain approaches. For example, if an internal automated security system frequently detects a certain type of leakage incident, the application of this system should be expanded and the system itself should not be frivolously replaced. If an analysis indicates that various incidents can only be prevented by internal manual control, it would make sense to increase manual control in this domain. Moreover, the source of the detection can be used to prove the efficiency of IS measures and to train awareness.

14) RECURRENCE RISK

A critical or high risk of recurrence signals the need for immediate action with less consideration of costs and effort. Incidents, which repeatedly present equal criteria, indicate that countermeasures are missing at all, the wrong countermeasures have been taken, or the taken countermeasures are ineffective. Hence, incidents with a low recurrence risk and equal criteria should never recur. Otherwise, they are not correctly assessed.

B. ANALYSIS OF DATA LEAKAGE INCIDENTS BASED ON ADVANCED CRITERIA

In the course of this work, the data breaches of PPI reported in 2014 are extended by the advanced criteria which are presented in the previous section. Using this extension provides further details in addition to the preliminary findings illustrated in Section II. In order to focus on incidents directly affecting DLP and ILP measures, the analysis does not contain records which are identified as hacks from outside. For extending the records a set of predetermined rules is applied. These rules are derived from known facts given in the records and assumptions about the affected data which are usually known and defined by an organization. For example, an organization classifies a name associated with medical or financial information as top secret.

As depicted in Figure 2, the source of the data breach was considered inside in 486 cases, outside in 245 cases, and unknown in 88 cases. The results, which are derived from the analysis based on the proposed criteria, reveal different numbers and further details. In order to recognize potential relations, it is required to consider the proportional distributions of participants, intentions, and access points which are shown in Figure 4. The number of unknown participants increases whereas the number of cases, which are classified as external only, has to be reduced due to inexact information. Furthermore, the significant number of incidents with multiple participants demonstrates deficiencies across multiple authorities. Incidents with a data access point inside an organization are most common. In these cases data leaks within a zone which can be monitored and protected. In addition, the results reveal that in over 60 % of the data breaches the participants use their correct identity and are authorized to access the data. The advanced criteria indicate that 273 data breaches, which is equivalent to approx. 33 %, are unintentional. Comparing this number to the result of the preliminary findings, which states that 214 data breaches were caused by insiders accidentally, demonstrates the need for improving awareness. The distribution of access modes shows that technological as well as non-technological measures are important when it comes to DLP and ILP.

As mentioned above, this work applies a set of rules for extending the data breaches by the proposed criteria. In this context, knowledge such as intellectual property and names

FIGURE 4. Distribution of advanced criteria applied to data breaches reported in 2014.

associated with credit/debit card numbers, medical data, or financial information is classified as top secret. Knowledge such as user names associated with passwords and names associated with passwords, account information, or social security numbers is assumed to be secret. Information such as credit/debit card numbers, medical data, or financial

information is categorized as secret, too. As depicted in Figure 4, the number of data breaches, which affect data classified as top secret and secret, is remarkable. Considering the large quantity of leaked knowledge, these incidents should be taken seriously since the facts point toward missing or malfunctioning IS measures.

Further deficiencies are disclosed by the high number of data breaches which involve DIU and DAR as well as endpoint devices and storage mediums. It is required to investigate whether protective measures for endpoint devices and storage mediums, such as data encryption and access control, are in place and fully functional. The small number of leakage incidents associated with DIM indicates that it is more complex to gather information from this data state. Furthermore, network security systems may not provide a notice if data breaches are automatically detected and blocked.

Leakage incidents related to data are missing in the category information value. This is due to the fact that the value of raw data is difficult to assess and data breaches related to raw data are hardly identified as such. Additionally, the analysis based on the advanced criteria demonstrates that a large amount of incidents involve visible and permitted communication channels. However, organizations could not prevent those data breaches although approx. 60 % of all leakage incidents are detected by the organizations themselves.

For a significant number of data breaches the recurrence risk has to be rated critical or high due to missing details about the incidents. It is not possible to reliably prevent the recurrence of a certain leakage incident in case of remaining questions such as: What did happen? When did it happen? How did it happen? Why did it happen? In general, the high proportion of the type unknown in the categories access mode, data state, communication channel, communication medium, communication mode, and incident detection proves that important details are missing in a variety of data breach records. This fact indicates the weaknesses of organizations when it comes to knowledge management and IS.

In summary, the advanced criteria for characterizing data leakage incidents demonstrate their significance by providing a variety of additional knowledge. Hence, these criteria are a recommendation for authorities which have to establish future data loss notification regulations and IS measures. Furthermore, the proposed criteria allow to identify own and common weaknesses in IS. On the one hand, these weaknesses refer to limitations of the implemented security measure such as an enterprise content-aware DLP solution. On the other hand, they demonstrate that applying a self-contained DLP solution is not sufficient. This is due to the fact that DLP solutions are limited to prevent technologically based data breaches and that they rely on a secure and applicable infrastructure. Therefore, various IS measures have to be in place in order to ensure their effectiveness. As a consequence, this article introduces a concept for establishing DLP and ILP within the scope of IS in Section V.

The analyses of information, which is extracted from the textual description included in the data breach records, disclose a further detail: Almost all incidents demonstrate a basic three-phase structure and a consistent incident sequence which is illustrated in Figure 5. Due to different phase characteristics, which depend on the user authorization and the predominant information security level of an organization, certain variations are identified.

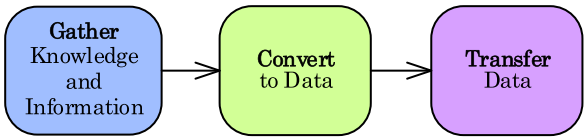

FIGURE 5. Basic structure of a data leakage incident.

The first phase towards an unwanted information exposure is information gathering which usually includes obtaining data access. If an unauthorized person shows conspicuous behavior, an incident can be prevented in this early stage. Qualified measures are a strict access control, a close supervision of failed attempts, and an appropriate reaction such as locking the user account after five failed login attempts. However, these methods can be challenging due to possible weaknesses in the scalable rights management, proper access control, and monitoring. The complexity involved in these fields of IS gives rise to potential failures.

After retrieving the desired information the affected data has to be transferred to a data medium or a system which is not monitored or supervised by, for example, a DLP solution. Due to the fact that control systems often prevent original data from being transferred, it might be necessary to convert the data. In case of small data amounts, such as a short list of user names and passwords, data can be converted by keeping the information in mind. In order to transfer a large amount of data out of the business premises of an organization it can be printed, encrypted, encoded, or fragmented. The data transfer itself can utilize covert channels, such as internet control message protocol (ICMP) tunnels, or unused fields in network protocols. In general, there are plenty of possibilities for converting data to a format which can bypass control systems and transfer the desired information.

IV. CRITERIA FOR CHARACTERIZING THE RELEVANCE OF ATTACKS

There is a wide range of attacks which can lead to the disclosure of information by data leakage. The relevance of a data leakage attack depends on the presented threat. A threat analysis has to be performed as part of the risk assessment in compliance with the ISO/IEC 27000 standards [17]. This analysis can be used to determine the risk of a thread with respect to

- the probability of its occurrence, and
- the possible impact of its occurrence.

Organizations have to consider data leakage attacks which represent a relevant threat with an unacceptable level of risk. The risk estimation can be quantitative, semi-quantitative, or qualitative. A quantitative estimation frequently presents

an accuracy which is hardly feasible, whereas a qualitative estimation can be reduced to, for example, high (probable), medium (possible), and low (improbable). In order to estimate the risk, measures for quantifying, comparing, and prioritizing have to be defined. Considering DLP, this work proposes to account the factors

- quantity,
- data value,
- complexity,
- effort, and
- detection risk

for the risk estimation. The quantity of the transferred data in correlation with the data value influences the effectiveness of a data leakage attack. For example, covert channels are a constant threat to DLP. According to an article which was published in 2006 [18], exfiltration methods, such as covert channels, can be classified by assuming that the covertness is proportional to the difference between the data volume to be transferred and the actual transmission rate. The article argues that it is more likely to detect a person stealing 10,000 pages of printed confidential information than to detect a person stealing 10,000 pages of confidential information stored on an electronic medium such as a USB drive. As mentioned above, there is a difference whether single bytes or several gigabytes can be transferred in a predetermined time interval. Nevertheless, a few bytes of data can result in a bigger threat to an organization than a gigabyte of data with a low data value. For example, a password, a personal identification number (PIN), or an amount of money can be stored in a few bytes. Therefore, the data value, which is composed of the data classification and the information value, is an important factor. This factor influences the relevance of the quantity.

A complex attack vector, which requires a deep understanding of technical coherences, seems not as probable in practice as an attack vector which can be successfully accomplished by a trainee. However, complex attack vectors are made accessible by tools such as software applications, software frameworks, executable scripts, and code examples. In general, an attack may be in need of preparations, e.g. to install software, to escalate privileges, or to obtain an authorized user account. Therefore, the complexity factor refers to the preconditions as well as to the complexity of an attack vector.

The effort of time and costs required to implement an attack vector is influenced by its complexity. On the one hand, it involves, for example, acquiring knowledge, investigating security measures, analyzing probabilities, influencing the environment, and obtaining authorized user account credentials. On the other hand, there are expenses for buying specific hardware and software. In order to be attractive, the object of an attack has to be worth the effort.

Another factor, the detection risk, should not be underestimated. An internal attacker not only risks instant dismissal but also commits a crime which can be prosecuted by criminal law as well as by civil law. It is important to inform employees about these facts in order to increase the inhibition level for stealing data. In general, the detection risk and the effort influence the motivation to abstract data from an organization. For example, a low detection risk and little effort seem to be encouraging factors for an attack. The consequences of a detection, such as mean damage, charges, or expenses, can increase the deterrent or can lead to extended effort for reducing the detection risk. Therefore, IS measures are important to influence the detection risk, the effort, and the complexity of an attack.

V. DLP AND ILP AS A CONCEPT OF INFORMATION SECURITY

There are several theories within the scope of IS and especially IT security, such as the Kurt Gödel's incompleteness theorem [19], the Alan Turing's halting theorem [20], and the Rice-Myhill-Shapiro theorem [21], which proof that IT security is a matter of probability. Furthermore, academic research recurrently demonstrates cases in which data or information leakage is unpreventable. A group of researchers, for example, recently demonstrated that it is even possible to retrieve data from isolated air-gapped systems by using their heat emissions [22]. Thus, various data breaches are inevitable.

A. THE HUMAN FACTOR

A decisive key factor within the scope of IS in organizations is the human factor. Human individuals introduce knowledge into organizations and create intangible and tangible assets by using data, information, and knowledge. In the context of DLP and ILP, individuals have to estimate the value of intangible assets. Furthermore, individuals correctly or incorrectly identify data, information, and knowledge worth protection, they calculate the security risks to the best of one's knowledge, they take appropriate security measures based on the risk estimation, they define regulations, and they comply or do not comply with these regulations. An organization can attempt to force its employees to comply with these regulations by using control mechanisms, surveillance, and monitoring. But this approach has been proven to be ineffective in several cases such as the incident of Edward Snowden [23]. DLP and ILP solutions show, as well as other surveillance technologies such as intrusion prevention systems (IPSs) and intrusion detection system (IDSs), certain deficiencies especially when it comes to covert or subliminal channels and steganography. The statements in [24], for example, describe a subliminal channel established between two communication endpoints which secretly communicate through messages clearly visible to a control point. The messages themselves contain no secret which can be identified as a secret by the control point. Furthermore, the messages can be authenticated by the communication endpoints allowing to detect malicious messages.

Moreover, individuals can unintentionally or intentionally leak data, information, and knowledge through a wide range of technological and non-technological communication systems. Due to the fact that there is no

never-known-to-fail method to prevent leakage and in order to prevent as many incidents as possible, an organization relies on the acceptance and the cooperation of its employees accordingly. Various research results, e.g. [25]–[27], indicate that employees are willing to accept computerized monitoring and continuous surveillance and to comply with IS policies and measures under certain conditions. According to [25], employees demand information about the recorded data, they prefer data not attributable to individual persons, they expect access limitations to this data, and they are concerned about the design and implementation of the surveillance system. Furthermore, the results presented in [26] indicate a strong positive correlation between the users' attitude and intention toward using IS solutions, the users' knowledge, and the users' experience with these solutions. Therefore, various factors, such as useable security, negative attitudes towards control mechanisms, as well as country specific regulations, have to be considered in order to ensure the acceptance and the cooperation of employees.

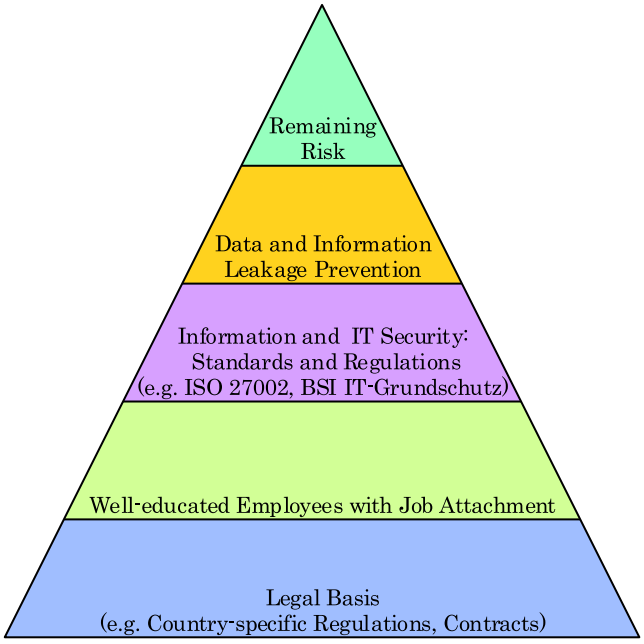

FIGURE 6. DLP and ILP as a concept of IS within the ILP pyramid [2].

B. THE ILP PYRAMID

The ILP pyramid, which is illustrated in Figure 6, was first mentioned in 2014 [2]. It is based on the assumptions that IS is a matter of probability and many aspects of IS have to be considered to reduce the probability of data and information leakage. The ascending levels of the ILP pyramid have the objective to minimize the probability of data and information leakage. This probability is represented by the remaining risk at the top of the pyramid.

A legal basis for permanent surveillance and monitoring has to be established in order to meet country-specific regulations. For example, the financial sector in Austria commonly expects clear agreements within contracts as well as non-disclosure agreements to prevent violations of security and supervisory measures which can be prosecuted by criminal law and civil law. The influence of the human factor on IS is addressed in the second level of the ILP pyramid. Control mechanisms, such as surveillance and monitoring measures, affect the trust and satisfaction of employees. Trustworthy and well-educated personnel are required to implement, configure, manage, monitor, and operate the technical installations within the infrastructure of an organization. Furthermore, employees and TBPs have access to data, information, and knowledge of an organization. Considering the number of data breaches which involve insiders, it is important to keep their competence, training, and awareness up to date.

The next level of the ILP pyramid takes compliance with IS standards and regulations into account. It is highly probable that various data breaches could have been prevented if the affected organizations would have been compliant with, for example, the ''BSI IT-Grundschutz-Kataloge'' (BSI IT Baseline Security Catalogs) [28] published by the German Federal Office for Information Security (BSI) or the ''Österreichische Informationssicherheitshandbuch'' (Austrian Information Security Handbook) [29]. These standards recommend methods, such as data encryption, access control management, and measures to guarantee the confidentiality and integrity of sensitive data, which correspond with the objectives of DLP and ILP. Therefore, compliance with IS standards and regulations, and gaining a high level of IS are prerequisites for DLP and ILP.

An ILP concept has to address the remaining organizational and technical issues which are specific to DLP and ILP. In general, enterprise content-aware DLP solutions, such as the products of McAfee [9], Symantec [10], Digital Guardian formerly known as Verdasys [11], and Websense [12], rely on certain IS measures to be established in order to reduce the risk of technologically based data breaches. Relevant examples for such IS measures are physical access controls and well-conceived access priviledge concepts. Under certain conditions these solutions are able to identify, classify, and protect data. But data leakage, which is caused by hard copies of information and knowledge or by pictures of monitor screens taken non-authorized, cannot be prevented. Furthermore, a recent study argues that evaluated DLP solutions can indeed prevent accidental file uploads over Hypertext Transfer Protocol (HTTP) but they are not able to prevent basic data leakage caused by internal attackers or malware [30]. Another article indicates that industrial DLP solutions are mainly utilized to prevent accidental leakage incidents [31]. Therefore, ILP concepts have to exceed the implementation of a self-contained DLP software solution by establishing the underlying levels of the ILP pyramid.

However, even if all levels are well considered and implemented there is a remaining risk which is represented by the top level of the ILP pyramid. This risk cannot be eliminated due to certain unpreventable data breach scenarios.

VI. CONCLUSION

In the context of IS, the assumption ''dumbest assumable user (DAU)'' as well as absolute confidence in the control, monitoring, and surveillance mechanisms have to be considered risky. The analysis of data breaches reported in 2014 demonstrate that only a part of the data breaches associated with insiders were unintentional. Considering that administrators of IT security systems and common users with appropriate knowledge are able to cause data breaches, it is more advantageous to expect the ''smartest assumable attacker (SAA)''. In order to gain further knowledge about reported data breaches, this work proposes advanced criteria for characterizing data leakage incidents as well as certain criteria for characterizing the relevance of attacks. They prove to be a helpful instrument to indicate the significance of successful IS measures and to reveal weaknesses. The analysis of data leakage incidents based on these advanced criteria illustrate that the human factor is a decisive key factor within the scope of IS. Organizations rely on the acceptance and the cooperation of their employees because there is no never-known-to-fail method to prevent leakage. Furthermore, state of the art enterprise content-aware DLP solutions are not able to reliably protect information assets. This is due to the fact that these solutions depend on certain IS measures to be established in order to reduce the risk of technologically based data breaches. Therefore, this work introduces a coherent concept consisting of various elements for establishing DLP and ILP within the scope of IS.

REFERENCES

[1] Wikimedia Foundation, Inc. *Data Loss Prevention Software*. [Online]. Available: https://en.wikipedia.org/wiki/Data_loss_prevention_software, accessed Oct. 25, 2015.

[2] B. Hauer, ''Data leakage prevention—A position to state-of-the-art capabilities and remaining risk,'' in *Proc. 16th Int. Conf. Enterprise Inf. Syst. (ICEIS)*, vol. 2. Lisbon, Portugal, Apr. 2014, pp. 361–367.

[3] *Information Technology—Vocabulary—Part 1: Fundamental Terms*, Standard ISO/IEC 2382-1:1993, Jun. 2010.

[4] K. North, *Wissensorientierte Unternehmensführung—Wertschöpfung durch Wissen*. Wiesbaden, Germany: Gabler Verlag, 2011.

[5] CWE. *CWE-200: Information Exposure*. [Online]. Available: http://cwe.mitre.org/data/definitions/200.html, accessed Oct. 25, 2015.

[6] M. E. Maron, ''Automatic indexing: An experimental inquiry,'' *J. ACM*, vol. 8, no. 3, pp. 404–417, Jul. 1961.

[7] E. Ouellet, ''Magic quadrant for content-aware data loss prevention,'' Gartner, Inc., Stamford, CT, USA, Tech. Rep., Sep. 2013.

[8] T. Raschke, ''The forrester wave: Data leak prevention, Q2 2008,'' Forrester Res., Cambridge, MA, USA, Tech. Rep., Jun. 2008.

[9] McAfee, Inc. (Oct. 2015). *McAfee Total Protection for Data Loss Prevention*. [Online]. Available: http://www.mcafee.com/in/products/total-protection-for-data-loss-prevention.aspx

[10] Symantec Corporation. (Oct. 2015). *Symantec Data Loss Prevention*. [Online]. Available: http://www.symantec.com/data-loss-prevention

[11] Digital Guardian. (Oct. 2015). *Digital Guardian Platform*. [Online]. Available: https://digitalguardian.com/products/digital-guardian-platform

[12] Websense, Inc. (Oct. 2015). *TRITON APX*. [Online]. Available: http://www.websense.com/content/triton-apx.aspx

[13] M. Hart, P. Manadhata, and R. Johnson, ''Text classification for data loss prevention,'' in *Privacy Enhancing Technologies* (Lecture Notes in Computer Science), vol. 6794. Berlin, Germany: Springer, 2011, pp. 18–37.

[14] Y. Park, S. C. Gates, W. Teiken, and P.-C. Cheng, ''An experimental study on the measurement of data sensitivity,'' in *Proc. 1st Workshop Building Anal. Datasets Gathering Exper. Returns Secur. (BADGERS)*, Salzburg, Austria, Apr. 2011, pp. 70–77.

[15] Open Security Foundation. *DataLossDB*. [Online]. Available: http://www.datalossdb.org, accessed Sep. 15, 2015.

[16] J. Rowley, ''The wisdom hierarchy: Representations of the DIKW hierarchy,'' *J. Inf. Sci.*, vol. 33, no. 2, pp. 163–180, 2007.

[17] *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*, Standard ISO/IEC 27000:2012, Sep. 2012.

[18] A. Giani, V. H. Berk, and G. V. Cybenko, ''Data exfiltration and covert channels,'' *Proc. SPIE*, vol. 6201, p. 620103, May 2006.

[19] K. Gödel, ''Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I,'' *Monatshefte für Mathematik und Physik*, vol. 38, no. 1, pp. 173–198, 1931.

[20] A. M. Turing, ''On computable numbers, with an application to the Entscheidungsproblem,'' in *Proceedings of the London Mathematical Society*, 1936, vol. 42. no. 2, pp. 230–265.

[21] H. G. Rice, ''Classes of recursively enumerable sets and their decision problems,'' *Trans. Amer. Math. Soc.*, vol. 74, no. 2, pp. 358–366, 1953.

[22] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici. (Mar. 2015). ''BitWhisper: Covert signaling channel between air-gapped computers using thermal manipulations.'' [Online]. Available: http://arxiv.org/abs/1503.07919

[23] G. Greenwald, E. MacAskill, and L. Poitras, ''Edward Snowden: The whistleblower behind the NSA surveillance revelations,'' *Guardian*, Jun. 2013.

[24] G. J. Simmons, ''The prisoners' problem and the subliminal channel,'' in *Advances in Cryptology*. New York, NY, USA: Springer, 1984, pp. 51–67.

[25] R. A. Grant and C. A. Higgins, ''Computerized performance monitors: Factors affecting acceptance,'' *IEEE Trans. Eng. Manag.*, vol. 38, no. 4, pp. 306–315, Nov. 1991.

[26] P. A. Wang, ''Information security knowledge and behavior: An adapted model of technology acceptance,'' in *Proc. 2nd Int. Conf. Edu. Technol. Comput. (ICETC)*, vol. 2. Shanghai, China, Jun. 2010, pp. V2-364–V2-367.

[27] A. Al-Omari, O. El-Gayar, and A. Deokar, ''Security policy compliance: User acceptance perspective,'' in *Proc. 45th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Maui, HI, USA, Jan. 2012, pp. 3317–3326.

[28] *BSI IT-Grundschutz-Kataloge*. Bonn, Germany: Bundesamt für Sicherheit in der Informationstechnik (BSI), Apr. 2013.

[29] *Österreichisches Informationssicherheitshandbuch*, Bundeskanzleramt Österreich (BKA), Schweizer Informatikstrategieorgan des Bundes (ISB) und Zentrum für sichere Informationstechnologie—Austria, Wien, Austria, Nov. 2012.

[30] D. Gugelmann, P. Studerus, V. Lenders, and B. Ager, ''Can content-based data loss prevention solutions prevent data leakage in Web traffic?'' *Trans. Amer. Math. Soc.*, vol. 13, no. 4, pp. 52–59, Jul./Aug. 1953.

[31] A. Shabtai, Y. Elovici, and L. Rokach, *A Survey of Data Leakage Detection and Prevention Solutions* (SpringerBriefs in Computer Science). New York, NY, USA: Springer, 2012.

BARBARA HAUER received the M.Sc. degree in secure information systems (Sichere Informationssysteme) from the University of Applied Sciences Upper Austria, Hagenberg, Austria, in 2006. After her master studies, she started to investigate data and information exposure threats in the context of information security. She is currently pursuing the Ph.D. degree in informatics with Johannes Kepler University of Linz, Austria. Her research interests are focused on data leakage prevention (DLP), information leakage prevention (ILP), and the human factor in information security.