Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

People, Process, and Technologies Impact on Information Data Loss

Organizations lose proprietary information daily due to hackers, insiders, or business partners. Most organizations assume this issue can be addressed with technology alone, but that is not realistic. This paper will demonstrate how focusing holistically on people, processes, and technology can reduce the impact of data loss. People can be trained to recognize threats such as phishing and social engineering. Processes can address the issue through policies and procedures. Technology can be implemented to monitor and p...

Copyright SANS Institute
Author Retains Full Rights

AD

Entrust
< Let's Talk

INFORMATION ASSURANCE AND SECURITY INTEGRATIVE PROJECT

PEOPLE, PROCESS, AND TECHNOLOGIES IMPACT ON INFORMATION DATA LOSS

PAUL JANES

November 07, 2012

Abstract

Organizations lose proprietary information daily due to hackers, insiders, or business partners. Most organizations assume this issue can be addressed with technology alone, but that is not realistic. This paper will demonstrate how focusing holistically on people, processes, and technology can reduce the impact of data loss. People can be trained to recognize threats such as phishing and social engineering. Processes can address the issue through policies and procedures. Technology can be implemented to monitor and prevent data leaving a business. To be successful, an organization will need support from C level leadership, management will need to identify critical data, and IT, together with Legal and HR, should collaborate on the processes and technological solutions.

CONTENTS

Abstract ii

Table of Figures vii

List of Tables viii

Chapter 1 Introduction 1

Background 1

Chapter 2 How Data Loss Occurs 3

Insider Threat 4

Insider IT Sabotage 4

Insider Theft of Intellectual Property 5

Insider Fraud 6

Human Error 6

External Threat 7

Partner Threat 8

Environmental and Physical 8

Chapter 3 Review of Recent Data Loss Incidents 10

2011 Incidents 11

Significant Data Loss Events 11

2012 Incidents 12

Significant Data Loss Events 12

Chapter 4 How to Address the Issue of Data Loss 14

People 14

Background Checks 14

Training and Awareness 15

Process 16

Incident Response Process 16
Governance Process 17
Investigations Process 17
Policy 18
Data Classification 19
Data Retention and Destruction 20
Sharing Corporate Data with Business Partners & Third Parties 21
Password Policies 22
Procedures 22
Technology 23
Data Loss Prevention 23
Monitoring the Network 24
Discover Confidential Stored Data 24
Protect Data 25
Encryption 26
Marking and Classification Systems 27
Secure Web Gateway 28
Digital Rights Management 28
Security Information and Event Management (SIEM) 29
Chapter 5 How to Address Data Loss within an Organization 30
Governance 30
Program Development 31
Risk Assessment and Controls Analysis 31
Project Identification 32
Vendor Selection 33

Deployment Strategy 34
DLP Deployment 34
Steering 34
Staffing 34
Policies 35
Technical Deployment 35
Rule Creation 35
Rule Approval 36
Rule Deployment 36
Scanning 36
Endpoint 37
DLP as a Control 37
Integration 37
Other Implementations 38
Marking Tool 38
DRM 38
Secure Email Gateway 39
SIEM 39
Control Gap Analysis and Hardening 39
Policy, Process, Procedures Review and Awareness Training 39
Risk Management 40
Chapter 6 Legal and Ethical Implications 42
Ethics 43
Chapter 7 Conclusion 44
References 45

Table of Figures

Figure 1.Threat agents over time by percent of breaches. (Verizon, 2012, p.16) 3

Figure 2.Data loss Statistics. (Open security foundation, 2012).....10

Figure 3. Risk Assessment and Controls Analysis.....32

Figure 4. Project List.....33

Figure 5. Risk Management Cycle.....41

List of Tables

Table 1 *Data Classification Example (Fine, 2011)* 19

Table 2 *Destruction Techniques* 21

Chapter 1

Introduction

Organizations have always had contend with issue of data loss; however, with the advent of the computer and worldwide connectivity, the problem has become magnified. With new technological capabilities come new threat vectors to corporate data. Mobile computing has introduced the new problem of corporate data being stored on mobile phones and tablets. BYOD has for the first time introduced the threat of corporate data on user's personal devices. Cloud storage has introduced storing corporate data externally with companies such as Dropbox, YouSendIt, and Box.net. These all create vulnerabilities that can be exploited.

Often the data lost is of a confidential nature. In a recent Ponemon study on confidential documents at risk, "Ninety percent of organizations represented in this study experienced the leakage or loss of sensitive or confidential documents over the past 12-month period" (Ponemon Institute, 2012). As a result, organizations have experienced significant financial impacts. In 2011 alone, the average organizational cost of a data breach was 5.5 million dollars (Ponemon Institute, 2012).

If action is not taken to reduce the impact of data loss an organization could easily go out of business. "Ideas, patents, and inventions are routinely stolen. Companies have closed before realizing that the sudden competition that ran them out of business resulted from their own stolen information" (Grimes, 2012). To reduce this risk, organizations must take action by focusing their efforts on people, process, and technology.

Background

Organizations too often believe that data loss is solely an IT problem and that technological solutions can address the issue. Unfortunately, technology is not the magical

solution. According to a recent Ponemon study on confidential documents at risk, , “59 percent say their organizations controls are ineffective at monitoring employees, contractors or other insiders who access these confidential documents” (Ponemon Institute, 2012). Users who have access to the data are often the root cause of the data loss. Employees opening an email which launches malicious code, data on a lost thumb drive, sending confidential data via email, or innocently connecting to a malicious website all demonstrate that the human element is a major factor in the data loss problem and must first be controlled before technology can make a difference.

The lack of appropriate processes is another factor resulting in data loss. If there are no data usage policies or secure transmission procedures in place data will be lost (Ernst & Young, 2011). Coupled with the lack of data usage monitoring and perfect storm is created.

Chapter 2

How Data Loss Occurs

All data breaches start with a precipitating event which results in data loss. "Entities that cause or contribute to an incident are known as threat agents" (Verizon, 2012, p. 16). These threat agents vary and have different approaches. "Actions performed by them can be malicious or non-malicious, intentional, or unintentional, causal or contributory, and stem from a variety of motives" (Verizon, 2012, p. 16). Verizon identifies, "three primary categories of threat agents – External, Internal, and Partner" (Verizon, 2012, p. 16). Figure 1 below shows the threat agents over time by percent of breaches:

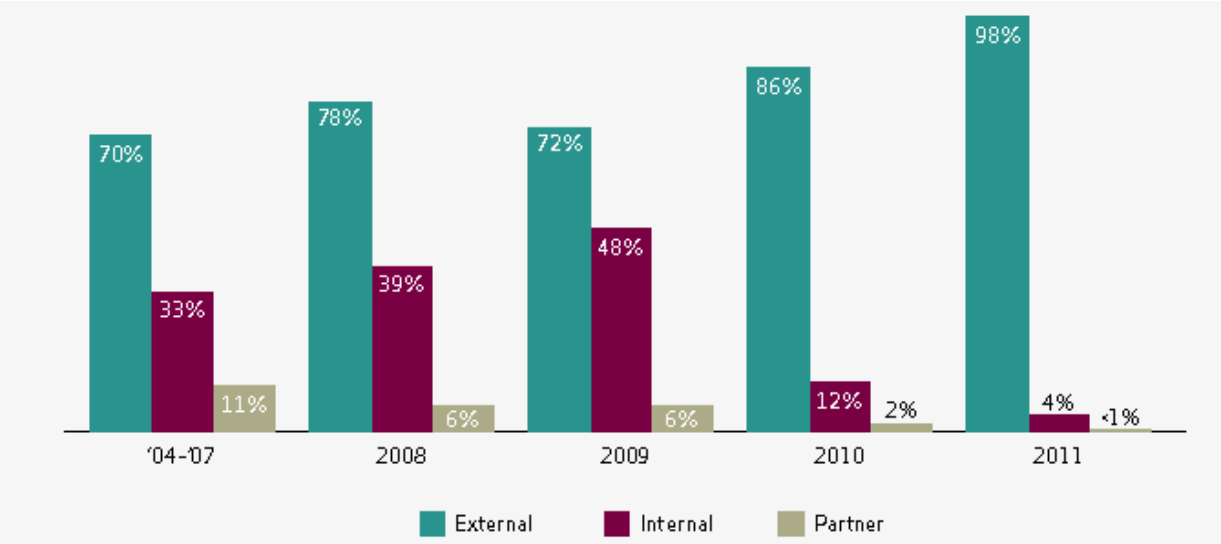

Figure 1. Threat agents over time by percent of breaches, by (Verizon, 2012, p.16)

Insider Threat

The insider threat involves individuals who work and have access to resources on the corporate network. They have physical access to the building, printers, fax machines, mail rooms, and possibly even the data center. This threat can the most difficult to track as users may actually have authorization to access the data in order to complete their jobs. In order to better understand this threat, CERT has identified three main categories which include insider IT sabotage, insider theft of intellectual property, and insider fraud (Capelli, Moore, & Trzeciak, 2012, p. 1). A fourth category that will also be discussed is human error.

Insider IT Sabotage

Insiders who have advanced rights to systems can be considered very dangerous to an enterprise. These individuals have the ability to delete business information, destroy backup tapes, install viruses, make modifications to public facing websites, and shut down systems (Capelli et al., 2012, p. 3).

As Capelli, Moore, and Trzeciak state:

> Insider IT sabotage is typically committed by technical users with privileged access, such as system administrators, database administrators, and programmers. The motivation in these crimes is usually revenge for a negative workplace event, and the crimes are often setup while still employed, but executed following termination. (Capelli et al., 2012, p. 1)

An excellent example of insider threat occurred when a network administrator held the city's network passwords hostage. "After being reprimanded for poor performance and for threatening a coworker, he was reassigned to a different job. He refused to provide the passwords to his replacement, however, and was subsequently terminated, then arrested" (Capelli et al., 2012, p. 3). The network cited belonged to the city of San Francisco and is best known as the

Terry Childs case. Childs "was charged with 4 counts of tampering with a computer network" (McMillan, 2008, p. 1). The cost to the city of San Francisco was over $200,000 and is proof of how one person with privileged access can wreak havoc from the inside (McMillan, 2008, p. 2).

Insider Theft of Intellectual Property

Individuals who work on the inside often have the opportunity to use information systems to steal intellectual property. "This category includes industrial espionage involving insiders; information stolen often includes proprietary engineering designs, scientific formulas, source code, and confidential customer information" (Capelli et al., 2012, p. 5). Thefts of this nature can and do cripple organizations financially and competitively in the market place.

An excellent example of this threat occurred when a sales representative was approached by a competitor with a job offer. As Capelli, Moore, and Trzeciak describe:

> For the next two months, the sales rep emailed proprietary information from his current employer to his home, including customer lists, quotes, customer passwords, marketing and sales plans, material costs and profit margins, and a computer program used to configure quotes for customers. He then visited his potential employer and used a stolen password to access a secure area on his current employer's web site. This access enabled the competitor to access confidential information regarding customer orders, quotes requested, and more. The next day, he received a formal employment offer. He sent an email accepting the offer, and included a copy of the program he had emailed to his home earlier. Next, he deleted the contents of his hard drive at work, thinking that would destroy the evidence of his crime, and turned in his resignation. (Capelli et al., 2012, p. 5-6)

The cost to this company was not only losing its competitive edge in the marketplace but also the loss of customer confidence in the organization to keep their information secure.

Insider Fraud

Insider fraud can be defined as employees accessing information systems with the intent to modify or delete the data for financial gain. This can entail selling personal information such as credit card numbers, social security numbers or health insurance ID numbers, users modifying records; or stealing money directly from a bank, store, or the federal government (Capelli et al., 2012, p. 4). This threat will often go unnoticed for long periods of time depending on how smart the insider is; small changes often go unnoticed until an audit.

A computer manufacturer issued a recall notice for its product and subsequently hired a third party company to fulfill the claims. A staff member needing money for his ailing parents created false claims; had the items shipped to his personal address and to his family member's addresses; then sold the received parts for profit. (Capelli et al., 2012, p. 4-5). Capelli, Moore, and Trzeciak went on to state:

> Over a 20 month period, the manufacturer sent more than 90 shipments containing 500 products with a retail value of more than $8 million to the addresses supplied by the malicious insider. He then sold 90 of the products on an Internet auction site for more than $500,000. He was arrested, convicted, and ordered to pay more than $8 million in restitution, plus serve 51 months in prison. (Capelli et al., 2012, p. 4-5)

Human Error

Often users simply make mistakes and as a result data is lost. Users inadvertently send sensitive email to the wrong email address, lose laptops, usb drives, smart phones, print outs, or backup tapes with proprietary or protected data while traveling or in transit to an outside meeting

(Websense, 2011). These incidents happen quite frequently and many are documented in the media. According to Websense:

> A private doctor's office in Chattanooga, Tennessee, revealed it had waited a month before notifying 1, 711 patients that their personal data had been lost on a usb stick that was being used to back up patient data in case of a computer crash. (Websense, 2011, p. 3)

Data is lost in many different ways by trusted individuals on the inside. These trusted individuals, whom access is often not questioned, can cause significant data and financial loss as noted in the previous examples.

External Threat

The external threat originates from outside the organization. These threats are carried out by "former employees, lone hackers, organized criminal groups and government entities" (Verizon, 2012, p. 16). Much of the recent activity seen has been with Hactivist groups such as Anonymous and LulzSec.

A recent example of Hactivism with the group Anonymous and Symantec clearly defines the impact these threats have to an organizations bottom line. "Symantec revealed in a white paper that Anonymous stole PCAnywhere's source code in 2006 and could use that information to create vulnerabilities" (Sniderman, 2012). This breach required significant work by Symantec to supply free upgrades and patches to its customers.

The 2011 Sony breach by the LulzSec group exemplifies how these external threats directly impact a corporation and its consumers. According to Reuters, "following the breach, LulzSec published the names, birth dates, addresses, emails, phone numbers, and passwords of thousands of people who had entered contests promoted by Sony, and publicly boasted of its

exploits" (Reuters, 2012). This breach cost Sony over $600,000 according to reports (Reuters, 2012).

Partner Threat

Partner threat is based on business relationships with third parties with whom data is shared and lost due to human error or fraudulent activity. "This includes suppliers, vendors hosting providers, outsourced IT support, etc. A level of trust and privilege is usually implied between business partners" (Verizon, 2012, p. 16). This form of data loss is difficult to control as once the data leaves the organization oversight is lost. According to Verizon's report:

> Three instances of partner threat have been identified in Verizon's 2012 report. A publishing error was identified as the primary cause in the first two; the partner accidently posted sensitive data to a public-facing website. The third partner-sourced breach involved deliberate malicious misuse motivated by financial gain. A third party database developer identified SQL vulnerability while performing contract work and abused this knowledge in order to compromise the hiring corporation. (Verizon, 2012, p. 22)

Whether it be intentional or not, data loss still occurs and can cause an organization significant financial and intellectual loss. Corporate reputations can be jeopardized by these breaches and as a result a lost consumer confidence in the brand.

Environmental and Physical

Data loss can also occur due to environmental factors such as electrical storms, tornadoes, hurricanes, earthquakes, and floods. In these events damage occurs to entire cities where data centers are often destroyed. These events can wreak havoc on businesses if they do

not have adequate disaster recovery and business continuity plans in place. In 2011 two separate earthquakes hit New Zealand. As Mark Hayes stated:

> These tormenting earthquakes took precious lives, demolished homes and greatly affected established businesses. These incidents left critical conditions for the businesses; thereby leaving more than 3000 people jobless and almost 6000 businesses partially or completely destroyed. Many businesses that relied on electronic data suffered total or temporary data loss due to hardware damage and failure. This caused major setbacks for them but also made them realize the importance of data security and back up. (Hayes, 2011)

Physical issues such as hardware and software failures can also be a contributing factor to data loss. Storage systems fail which can introduce data loss situations along with data corruption. Software failures are often caused due to upgrades which go awry and result in either corrupt or worse case total destruction of data. These issues can all be addressed by having solid backups, adequate redundancy, and DR plans in place.

Chapter 3

Review of Recent Data Loss Incidents

Organizations have been historically reticent about reporting data breaches, however, over the past few years more and more organizations have been forthcoming. In 2012, security professionals have already seen a large number of reported incidents. The statistics in figure 2 show currently over 900 reported attacks. Projecting from this data, the total number of reported incidents for 2012 may well be over 1300 .Open security foundation, 2012, p. 1) It must also be noted that this may be just the tip of the iceberg as a significant number of breaches go unreported. Expect this to change as legislation is written requiring organizations to report any breach of data.

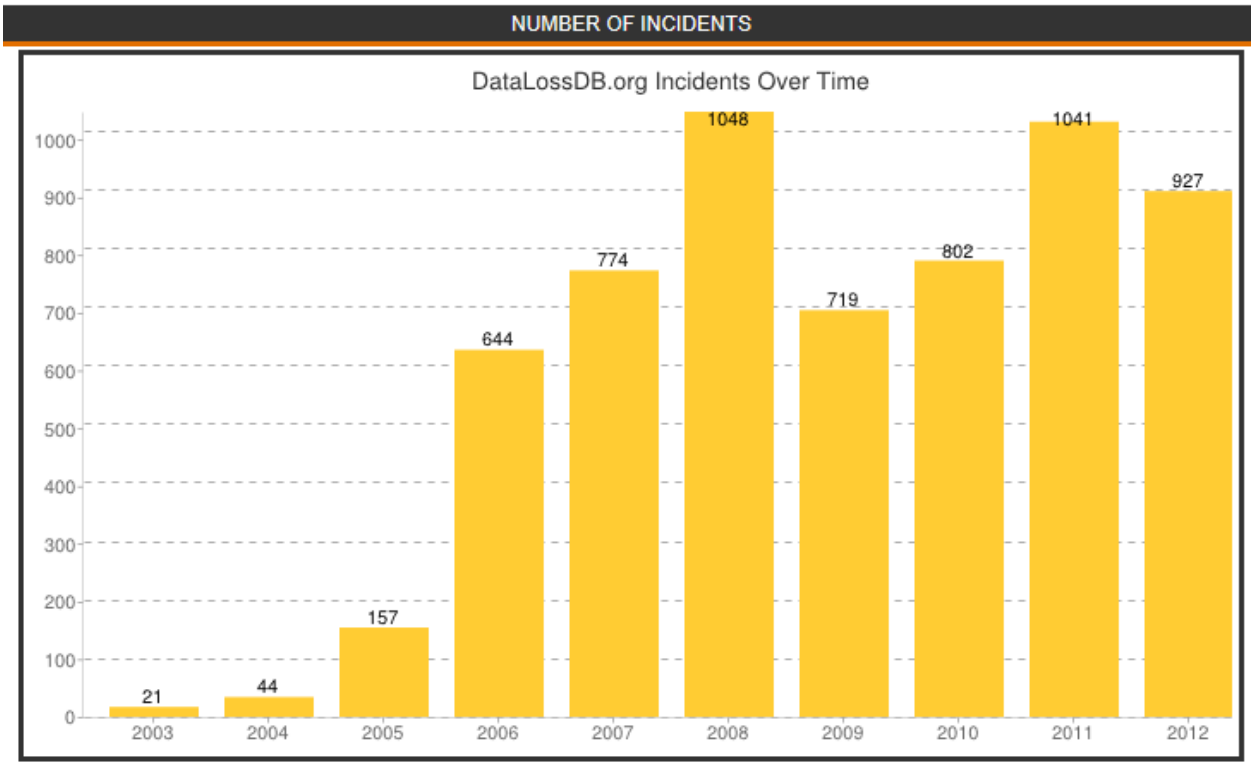

Figure 2. Dataloss Statistics, by (Open security foundation, 2012)

2011 Incidents

2011 was a year full of high profile data breaches. Breaches affecting organizations such as Sony, Espilon, HBGary Federal, and RSA Security were all made public (Rashid, 2011). These breaches were significant and resulted in volumes of data being lost or stolen. Many of these incidents were from external threats, namely the Hactivist groups Anonymous and Lulzec. Others were from insiders and from human error.

Significant Data Loss Events

As stated previously, Sony had over 101 million user accounts stolen which included personal information of all the users of its network (Rashid, 2011, p. 1). This was an external breach which was conducted by the group Anonymous. Sony had multiple exploitable vulnerabilities which made the attack extremely easy including lack of defense in depth measures, i.e. firewalls and intrusion prevention systems. Lessons learned from this incident convinced other companies to invest in additional security controls and solidly identified the need for a Chief Information Security Officer in larger corporations.

In another popular case, "external attackers breached e-mail marketing provider Epsilon's databases and waltzed off with e-mail marketing lists belonging to its clients, including Walt Disney, JPMorgan Chase, and Best Buy" (Rashid, 2011, p. 2). An estimated 60 million email addresses were taken in all (Rashid, 2011, p. 2). One great concern pertaining to this attack was that the large number of email addresses would be used in phishing or spear phishing attacks.

Security Organizations HBGary Federal and RSA also experienced data breaches at the hands of Anonymous. In the HBGary incident over 71,000 email addresses were stolen by exploiting poor passwords and unpatched servers (Rashid, 2011). Additional damage was done

as Anonymous deleted research and support documentation which led to the resignation of its CEO (Rashid, 2011, p. 1). RSA Security reported trade secrets stolen pertaining to their RSA SecurID two factor authentication product. As a result of a spear phishing attack on a small number of employees, malicious code was installed which enabled the breach of the internal network in order to obtain the intellectual property of RSA (Zetter, 2011).

Internal threats also occurred as in the case of Trilegiant Corporation. "A call center vendor's employee had been caught taking screen shots of customer data (names and debit or credit card numbers) with his phone camera" (Databreaches.net, 2011) . Insiders have access to information and can be very creative on how they go about taking it off company property.

Accidents do happen as shown in an incident at Wells Fargo. Due to an e-mailing error, "customer bank account numbers, balances, and transactions were accidently mailed to other customers in September paper statements" (Privacy rights clearinghouse, 2012). After further investigation, an issue with the printing system ended up being the reason for the data loss (Privacy rights clearinghouse, 2012). Human or system error can be a root cause of a major data loss incident.

2012 Incidents

2012 has already proven to be a big year for data loss. In 2012 there have been at least 6 major data breaches impacting organizations such as Zappos, Global Payment Systems, and LinkedIn (Dealing with data security, 2012). Each incident has resulted in significant data loss to the organization.

Significant Data Loss Events

2012 has had a number of data loss events caused by external parties hacking into each organizations network. Zappos reported a breach of over, "…24 million records, including

names, email addresses, phone numbers, last four digits of credit card numbers, and encrypted passwords" (Dealing with data security, 2012, p. 1). As a result users were forced to change their passwords and the organization realized significant embarrassment in the media.

In the Global Payment System breach, over 1.5 million credit card records were confiscated (Dealing with data security, 2012). This incident occurred after the company had just completed and passed an external PCI audit. This proves that compliance does not equate to a secure environment.

LinkedIn's social networking site was compromised exposing 6.5 million user passwords (Dealing with data security, 2012). The passwords were encrypted in an outdated format which with the current technical capabilities of black hats offered no protection. If LinkedIn had utilized best practices this event might not have occurred.

The insider threat case at UnitedHealthcare was made public when an "employee used the names, social security numbers, addresses, phone numbers, dates of birth, and Medicare health insurance claim numbers to steal the identities of at least 24 Idaho customers" (Privacy rights clearinghouse, 2012). Fraudulent activities such as this incur significant federal penalties due to HIPAA violations.

An incident earlier this year at Memorial Sloan-Kettering Cancer Center highlights the impact of human error. Five PowerPoint presentations were posted online which included imbedded HIPAA protected information on over 850 patients (Privacy rights clearinghouse, 2012). Users must be aware of all the meta-data a document or presentation may contain before posting it publicly.

Chapter 4

How to Address the Issue of Data Loss

Organizations must realize that the threat of data loss is real, significant, and that all are vulnerable. In 2012 alone the average cost of a data breach was 5.5 million dollars (Ponemon Institute, 2012, p. 2). What can be done about this issue? No single modality can address this problem effectively. Organization must focus on people, process, and technology to minimize vulnerabilities.

People

Employees and contractors who have access to corporate applications, trade secrets, budget data, strategy, as well as personal data, the internet, and email, are the greatest risk to organizations when it comes to data loss. The advent of the cloud and the consumerization of IT has only compounded an already serious issue. According to Olavsrud, "Your sensitive data is only as secure as the weakest link in your organization, and in many cases the weak link is your employees. A properly established security awareness and training program can pay huge dividends" (Olavsrud, 2012).

Background Checks

Prior to handing a badge, user id, and laptop to a new employee, a thorough background check is required by HR to validate resume information. Education, positions held, and job history all need verification. Corporate Security should also be engaged in conducting a criminal background check. By performing this activity effectively HR can identify red flags and significantly reduce the risk of the insider threat.

Training and Awareness

Security Training and Awareness is a required element of any data loss strategy. Training and awareness should address common data loss threats such as phishing, email, web browsing, social engineering, social networking, Wi-Fi, and information protection. End users should be educated in how to utilize corporate assets in a secure manner by using the corporate VPN, encryption, and secure communications. In addition, users require on-going training on corporate information security policies, procedures, and guidelines that need to be followed.

Awareness training should also include heightened awareness of suspicious activity. Whether it be something identified in logs or simply observing a fellow employee taking pictures of a whiteboard or computer screen, these actions need to be reported and acted upon without the fear of retaliation. It is considered a best practice to have an anonymous hotline for employees to report such activity.

Rather than an in house approach, it is recommended that organizations make use of existing awareness training such as SANS Securing the Human. This provides organizations with various modules which cover the different threat vectors as well as taking into account compliance requirements (Sans, 2012, p. 2).

SANS approach is as follows:

> Awareness cannot be created in a vacuum. It is the third tier in a pyramid starting with policy and training. Policy, training, and awareness go together in the following fashion:
>
> - Policy tells the user what to do
> - Training provides the skills for performing it
> - Awareness changes their behavior (Sans, 2012, p1)

The training and awareness program should include metrics so that the organization can track the impact of the program on its users (Olavsrud, 2012). Each year the program should be reviewed in order to focus on problem areas and new threats. One should never assume that training and awareness is a one-time event, but instead is cyclical and needs to keep pace with corporate policies and the latest threat vectors.

Process

Process addresses the gap between people and technology and includes policy and procedures. These need to be incorporated into the training and awareness program to not only raise awareness but to also provide the instructions users should follow based on the specific circumstance. Processes should be reviewed on a yearly basis; in order to be effective they must be current and address the various threats to data loss.

Incident Response Process

Security is not an exact science where elements can be identified assuring 100% protection. Having a comprehensive plan in place to address an incident when it happens is critical. Organizations should have an incident response process and individuals who are trained on the various threats that may occur. Examples of threats that can be used in training are Denial of Service, Worm, Advanced Persistent Threat (APT), Botnet, and IT sabotage.

Processes and procedures should be in place that dictates actions that should be taken for each threat type. Training exercises should be conducted which validate the incident response team's effectiveness in handling each incident type and successfully identify, contain, eradicate, and recover from each incident in a timely manner. Handling incidents in a timely manner is critical as the longer an incident persists; the longer the organization is at risk of additional infection and data loss. At the end of each incident lessons learned should be collected along

with corrective actions enacted so that in future events the same mistakes are not made. If an organization does not have the resources to address incident response they should outsource to a third party which specializes in these matters.

Governance Process

Governance is often mistaken for the committee oversees the process. According to the definition supplied by Sourabh Hajela, "IT Governance is a process used to monitor and control key information technology capability decisions - in an attempt - to ensure the delivery of value to key stakeholders in an organization" (Hajela, 2009). This ensures that IT decisions deliver benefit to the business and are not just simply IT projects for the sake of IT. The business benefit of addressing data loss has to be taken into consideration in order to sustain competitive advantage and often an organizations existence.

Investigations Process

Before a data loss incident occurs, processes need to be developed in order to properly address the potential data loss incident. Each incident should be reviewed and directed to a responsible party for action and root cause analysis. Responsible parties in data loss incident cases can be Corporate Legal, HR, CISO, Data Privacy Officer, or Corporate Security. In most circumstances the group will work together but each have their separate roles in addressing the data loss incident. This process is critical especially if the incident ends up in litigation. If the processes are not documented and the chain of evidence is not adhered to, the data collected will not be admissible in court.

Many incidents may not show themselves through logging or other technical means and are instead reported through an anonymous hotline. A review is required in order to delegate the incident report to the responsible party for appropriate action as indicated. These cases may

require special handling as they may be from an eye witness account; further information and documentation will be required based on the notification.

Policy

Policy is the foundation of any information security program and is owned by senior leadership within an organization. Effective policies provide statements which include what is acceptable, not acceptable, and the consequences for policy violation such as loss of employment or legal action. These are items that users "**must**" follow. These are not guidelines or recommendations.

According to Symantec:

> The goal of corporate security policies is to define the procedures, guidelines and practices for configuring and managing security in your environment. By enforcing corporate policy, corporations can minimize their risks and show due diligence to their customers and shareholders. (Symantec, 2010)

Policies must be published so that everyone in the organization can easily access them. End users should be notified immediately when polices are changed and whenever a violation occurs for remediation. They also need to be reviewed at minimally on a yearly basis to ensure they are current and address the current threats and the security programs direction. A semiannual review is best practice as it forces organizations to revalidate current policies against the latest threats.

The most important aspect of any policy is that it must be enforceable. Controls should be put into place in order to enforce the policy. Monitoring or alerting systems must be maintained in order to identify violations and to inform the governing bodies who are responsible for taking action.

Data protection policies must address data classification and retention, sharing of corporate information with business partners and other third parties, and password policies in order to ensure successful protection.

Data Classification

Data classification is a critical element in enforcing data protection. The intent of classification is to address three questions according to Naomi Fine, Esq, "Is it confidential? Whose information is it? What kind of protection should I apply" (Fine, 2011)? The data protection policy must require that all documents be classified. It must include the classification system to be used as well so that users know what, how, and why they need to classify documents. Fine suggests the following classifications as seen in Table 1:

Table 1

Data Classification Example (Fine, 2011)

Classification	Example
Company Special Handling	Trade Secrets, and New Product Information not released to the public
Company Confidential	Project plans and Spending plans
Company Private	Includes employee or customers social security #s, birth dates, and addresses

Utilizing document features such as the header and footer in order to display the classification on every page is suggested. For applications which do not offer these features text

fields can be utilized instead. Third party vendors offer products that enforce the data classification such as Titus, NetApp, and Microsoft.

Data Retention and Destruction

Policies need to address how long data is retained in paper or electronic format. If the data is not available, it cannot be lost or stolen. This requires planning in order to address the various types of data. As McGann stated:

> Breaking down the data into logical segments makes the process manageable and achievable. Defining a plan that targets the highest-risk data first is essential. The highest-risk data environments are typically e-mail servers and legacy tapes. Your policy can initially focus on the riskiest data and continue down to lower-risk items. That approach makes a monumental task more manageable. (McGann, 2012, p.1)

Organizations should make use of the data classification system and add additional categories as required in order to create a data retention schedule that meets their needs. Legal should be consulted in the retention policy design as there are legal requirements that must be fulfilled based on the type of information.

Destruction should be covered in the data retention policy so that users know how to destroy data appropriately. By retrieving papers thrown into the garbage, dumpster divers can obtain corporate or personal data. Third parties can help to address data destruction, but for those who do not trust having their data destroyed by others, Table 2 includes a list of a few data destruction techniques that are available.

Table 2

Destruction Techniques

Material	**Technique**
Paper	Cross- cut shredder or incinerate
Hard drive	DOD software to overwrite data repeatedly or incinerate
Backup Tape	Incinerate

Sharing Corporate Data with Business Partners & Third Parties

Policies should be very clear on the requirements of sharing business data with external sources such as business partners, vendors, and customers. Addressing communications with business partners and vendors is normally done via the nondisclosure agreement (NDA). These agreements have a specified scope and duration so even with an NDA is in place it may not be appropriate to discuss specific content. According to Nolo:

> Nondisclosure agreements are one of the best ways to protect trade secrets -- valuable confidential information that businesses want to keep under wraps. That information could be a sales plan, a list of customers, a manufacturing process or a formula for a soft drink. By using a nondisclosure agreement, you can ensure that your secrets stay secret -- or have legal recourse if they are misused or disclosed to the wrong parties. (Nolo, 2012)

It is very important to work with both the procurement and legal departments to verify before entering into any agreement with a third party in which trade secrets are shared that there is adequate protection.

Password Policies

According to documented accounts in the media, a number of security breaches have occurred due to exploitation of weak passwords. This issue would be significantly reduced if users simply created unique passwords for their accounts and did not use passwords that include dictionary words or well-known matches such as 123456. Organizations should implement strong password policies such as

- Minimum password length of 10 characters
- Require passwords changes every 30 days
- Inability to reuse the last 10 passwords
- Utilize 3 out of four special characters such as numbers, lower case letters, upper case letters, or special characters
- Disallowing dictionary words
- Prohibiting the sharing of passwords

Other recommendations include guidelines where users are strongly discouraged from using their corporate password anywhere else on the internet including webmail, cloud based storage applications, or website passwords.

Procedures

Procedures are written step by step instructions in order to accomplish a specific task such as how to properly mark classified documents in Microsoft Word, Excel or Power Point. End users need this instruction to effectively complete important tasks for adequate data protection. Classifying documents is part of the policy but the procedure explains how it is accomplished.

Another procedure to provide users is how to correctly share documents with business partners. This may include use of an extranet site created for the interaction, use of a hybrid cloud solution to conduct file transfers, or simply encryption of the message.

These all relate back to policies that are written in order to protect data. When procedures are written on how to use technological solutions they become very helpful for users. It is also an excellent addition to the training and awareness program identifying where the procedures are located and when to use them.

Technology

The technological solutions available today to address data loss protection are very beneficial to an organization. Technology can be used to enforce policies, monitor and alert violations, and to provide data protection. Technological solutions can also be utilized as countermeasures to address the risk of data loss whether it is intentional or human error.

Data Loss Prevention

Data loss prevention (DLP) is a control which can be used in order to protect critical data from leaving the organization. Per SANS description:

> Data loss prevention refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. Over the last several years, there has been a noticeable shift in attention and investment from securing the network to securing systems within the network, and to securing the data itself. DLP controls are based on policy, and include classifying sensitive data, discovering that data across an

> enterprise, enforcing controls, and reporting and auditing to ensure policy compliance. (SANS, 2012)

DLP can be utilized as a countermeasure for data loss by implementing policies that monitor, discover, and protect the network or the endpoint itself.

Monitoring the Network

DLP can monitor data on the network and report on any incidents where critical or personal data is being sent outside the corporate network. Emails can be monitored for content or attachments which include confidential or personal data. For documents that are marked, a policy can be implemented that monitors any email, http or ftp outside the company. The protocols that can be monitored currently are SMTP, http, https, IM and ftp (Symantec, 2011)

Discover Confidential Stored Data

One issue that organizations face is identifying where sensitive data is located on the network. In order to protect information, an organization needs to know where it is located, who the appropriate owner is and when it was last accessed. Many vendors have DLP offerings such as McAfee, RSA and Symantec which are all at the top of the Gartner Magic Quadrant for Data loss prevention (Gartner, 2011). Symantec is the leader of the magic quadrants so references to their product offering will be utilized. Symantec's offering can:

> Scan essentially any data repository, including file servers, databases, and web sites. Comprehensive coverage means you get visibility of all sensitive data, so you can take measures to reduce the risk of data loss.
>
> When a sensitive file is found, a rich set of incident data is provided to the information security team about exposed confidential information, including file owner and location, file content, and file permissions. (Symantec, 2011)

Protect Data

The key to any data loss prevention is the ability to protect data from being sent externally. This addresses the human error component and the malicious user trying to send critical data outside the corporate network. Current offerings provide email, web, and endpoint prevention.

Email Prevention

Email prevention prevents content and attachments from being sent outside the network through the corporate email system. Symantec states, "Network Prevent for Email redirects, quarantines, or blocks outbound messages containing sensitive data" (Symantec, 2011, p. 1). This can also address email on smartphone and tablets which have become very popular in the workplace.

Web Prevention

Preventing data loss through the web is a critical capability. Symantec's DLP offering has the following key features which can be used to prevent data from leaving the network over the internet:

- Corporate web protection for smartphones and tablets running Google Android, Apple iOS, BlackBerry, Windows Mobile.
- Cloud and social media protection for Salesforce.com™, Facebook®, Twitter®, YouTube™, and LinkedIn®.
- Hosted web and security services support for Symantec.cloud, Google Apps™, and Microsoft® Online Services.
- Exclusive enhanced web blocking seamlessly strips sensitive data from web posts. (Symantec, 2011, p. 2)

Addressing the cloud, smartphones, tablets and other online services is key in today's environment where BYOD and the consumerization of IT is prevalent.

Endpoint Prevent

In addition to the network and email, Endpoint Prevent works on the laptop following the device no matter where it is located on the network or off. Endpoint Prevent can stop or alert based on data being downloaded or copied "to CD/DVD/USB/iPod®/Bluetooth®, and other removable media; communications over email, Instant Messaging (IM), and the Web; and support for virtual Citrix® environments" (Symantec, 2011). This provides complete control of all removable media as well as any web site interaction as noted in the web prevent product.

DLP can significantly reduce the threat of sensitive data being sent out over the corporate or outside network. This addresses insider threat as a result of human error as well as fraud. The impact of external threats is reduced by catching data before it leaves. DLP systems are not 100 %, but no solution will offer that percentage of security.

Encryption

Regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry (PCI), and Sarbanes-Oxley Act (SOX) are forcing organizations to make use of controls which enforce encryption. SANS defines encryption as follows:

> Encryption works by using a mathematical formula called a cipher and a key to convert readable data (plain text) into a form that others cannot understand (cipher text). The cipher is the general recipe for encryption, and your key makes your encrypted data unique. Only people with your unique key and the same cipher can unscramble it. Keys are usually a long sequence of numbers protected by common authentication

mechanisms, such as passwords, tokens, or biometrics (like your fingerprint). (The SANS Institute, 2011)

Encryption can be used on hard drives and removable media to protect data if the devices are lost or stolen. Keeping the data in an encrypted format protects it until the user logs in and enters his or her credentials. Many of the endpoint solutions today offer a form of endpoint encryption such as Checkpoint, McAfee, Symantec, and Trend Micro.

Encryption may be required when sending email to business partners or third parties. The problem with email encryption is that most offerings require the sender and receiver to have special software. This is not always feasible if a corporation does business with a large number of partners. In order to address this solution, a secure email gateway is required which can work with DLP implementation to send email in an encrypted format. Most offerings utilize a secure portal which stores the data until the recipient connects to the secure portal via https and accesses the email. These offerings do not require any software on the recipients end and is available to anyone with a standard browser (Symantec, 2010). Product offerings by Cisco, Proofpoint, Microsoft, Google, and McAfee are all leaders in the latest Gartner magic quadrant for secure email gateways (Gartner, 2012). With the use of this technology and DLP, Information Security departments can significantly reduce the insider threat.

Marking and Classification Systems

Classifying data has a major impact on data loss as it provides the mechanism to identify sensitive data which needs additional protections. Solutions are available today which actually require the end user to classify the document before it is saved. The key benefits of these tools are that they “allow users to classify documents; assist users to properly capture the sensitivity of

their information; and automatically apply visual markings which highlight the sensitivity" (Titus, 2012).

Products currently exist that classify office, email messages, and files stored in SharePoint and other databases. This system provides consistent classification practices that can enforce the requirements of an organizations classification policy. This also helps by adding additional metadata which can be read by other systems such as DLP so that content aware policies can be enforced.

Secure Web Gateway

Accessing internet web sites often result in malicious code being deployed to the local machine which can lead to possible data loss depending on the malicious payload. In order to reduce the risk organizations deploy secure web gateways. According to Gartner, "SWGs must, at a minimum, include URL filtering, malicious code detection and filtering, and application controls for popular Web-based applications" (Gartner, 2012, p.1). This capability protects users against known malicious websites which are updated like antivirus definitions. Sites can also add their own url filters to blacklist or whitelist web sites depending on the current need. The top leaders in the 2012 report are Cisco, BlueCoat, Websense, and Zscaler (Gartner, 2012, p. 2).

Digital Rights Management

The last threat to address through technology is the business partner threat. Once data is sent to a business partner corporations are reliant on them for securing the information. This is a very uncomfortable position to be in. NDA's protect from a legal perspective but is there a way to bypass this situation in the first place? Enterprise Digital Rights Management offers protection wherever the file is located. According to Watchdox:

> WatchDox enables organizations to access, share and control their critical files wherever they go: On any tablet, smart phone, or PC, even those beyond the IT department's control. The WatchDox enterprise file centric security platform allows organizations to collaborate with partners, adopt to bring your own device (BYOD) initiatives, and control or wipe their files remotely, all while providing their users a superior experience across every device. (Watchdox, 2012)

One of the great capabilities of Enterprise Digital Rights Management is the capability to control what a user can do with a document. Owners can enforce rules that allow or disallow printing, editing, cut-paste, enforcement of watermarks, restriction on the ability to forward or attach in an email, and actually set an expiration date on the file so that at a set time the file is no longer legible (Watchdox, 2012). With this solution or control in place the business partner threat is considerably reduced. Solutions currently are available from SealedMedia and Watchdox.

Security Information and Event Management (SIEM)

An abundance of log data is being created on a daily basis by event logging systems, firewalls, proxies and other network devices. As Gartner states, "…customer's need to analyze security event data in real time for internal and external threat management, and to collect, store, analyze and report on log data for regulatory compliance and forensics" (Gartner, 2012). Organizations can implement this themselves or make use of managed services from organizations such as AT+T, Verizon, and Symantec. If the organization does not have adequate staffing, the managed service can provide the technical expertise that is required. Three of the leaders in this year's magic quadrant are HP, IBM, and McAfee (Gartner, 2012, p. 2).

Chapter 5

How to Address Data Loss within an Organization

Governance

Prior to embarking on the requirements for a data loss prevention program, senior leadership must commit and provide the appropriate resources and funding. Keeping sustained focus on the issue and addressing the needs of the organization based on cost, time, capability, and business benefit is the key. Without governance, a data loss protection program will fail based on the effort required.

Business leaders are a critical aspect to any data loss prevention program as they are the often the data owners. It is paramount that business leaders identify the data which is most critical to them in order for IT to implement secure solutions surrounding that data. This is not an easy task but considering the possible ramifications to the business such as lost competitive advantage, reputation damage, or loss of revenue it is worth the effort.

ITs role is to review and present projects for approval based on the needs of the organization. Looking for business benefit, cost savings, or other benefits which will account for the justification in project spend. Organizations may have the CFO review all spend presented by IT which without valid justification will be denied.

Best practices in IT governance often follow some sort of framework. According to Price Waterhouse Coopers:

> Ninety five per cent of the organizations seek aid and guidance from the major and well-known frameworks such as CobiT and ITIL. The fact that these frameworks are seldom separately used but rather combined with each other and/or other lesser known

> frameworks (such as CMMI, and PRINCE II) leads us to believe that most organizations do tailor the standards to their own needs.
>
> In addition, we have observed that many organizations focus first on getting the basics of IT Governance correct, i.e. installing the right governance bodies and committees, assigning accountability, and opening communication channels between business and IT. (Pricewaterhousecoopers, 2007, p.27)

Metrics are important for any process which has this visibility within an organization. Metrics should include cost, time, and business benefits. A balanced scorecard can be produced which allows the organization to monitor activities currently underway.

Program Development

With governance in place the next requirement is an effective Data Loss Prevention Program to address data loss concerns for the organization. The successful project manager will ideally have 7-10 years' experience, preferably a PMP certification, and the ability to manage multiple projects simultaneously as well as excellent time management skills and a thorough understanding of risk and resources management. Once this role has been filled the risk assessment and controls analysis can be started.

Risk Assessment and Controls Analysis

Before the project portfolio is defined a current risk assessment is required which will identify the risks to the organizations data. Risks will be reviewed against existing controls and prioritized based on impact and probability scores. This is a critical element as this identifies the areas in which focus and funding is required in order to create the project list. This is the time time to engage a third party to conduct penetration testing to locate weaknesses in existing controls and identify gaps in order to assess the current state of threat protection. Once complete

a risk assessment and controls analysis report can be produced. Figure 3 is an assessment based on the threats identified earlier:

Existing Threat	Risk Ranking	Existing Controls or Countermeasures	Effectiveness of Controls	Controls Required
Intellectual Property	10	Policies, Encryption, Classification System, Antivirus, Firewall, Proxy Server, Background Checks, Training and Awareness, and	L	DLP,DRM, Marking,
Human error	9	Policies, Background Checks, training and awareness, Spam Filtering, Encryption, Endpoint Protection, Firewall, Proxy Server, Secure Web Gateway	M	DLP, DRM, Marking
Business Partner	8	NDA, Encryption, Training and Awareness	M	Secure Email Gateway, DRM, Marking
Insider Fraud	7	Policies, Logging, Background Checks, Incident Response, Investigations, training and awareness	L	DLP, SIEM, Marking
IT sabotage	6	Policies, Log Management, Background Checks, Incident Response, Investigations, Training and Awareness	L	DLP, SIEM,
Environmental & Physical	5	DR Plan, BC Plan, Backup Procedures, Hardware monitoring, Policy, and training	H	

Figure 3. Risk Assessment and Controls Analysis.

Focusing efforts based on the prioritized list creates the foundation required in order to begin scoping out the projects that will be part of the current program. Internal SME's will be required in order to identify the requirements for each of the controls and in some cases outside consulting may be required where there is no internal expertise.

Project Identification

Decisions would be made to implement DLP, a secure email gateway, a marking tool, and SIEM based on the risk assessment and controls analysis. Another project would be required outside of these technologies in order to update processes, procedures, policies, and awareness training. If the controls analysis identifies weaknesses in existing controls, another project may

be required in order to address the vulnerabilities. If budget allows all 7 projects would be added to the portfolio for the data loss prevention program. See figure 4 for the entire list.

Project #	Description
1	DLP - RFP, Vendor selection, Proof of Concept, and Deployment
2	DRM - RFP, Vendor selection, Proof of Concept, and Deployment
3	SIEM - RFP, Vendor selection, Proof of Concept, and Deployment
4	Marking tool – RFP, Vendor selection, Proof of Concept, and Deployment
5	Secure Email Gateway - RFP, Vendor selection, Proof of Concept, and Deployment
6	Control Gap Analysis Validation and Hardening
7	Policy, Process, Procedures Review, and Awareness Training

Figure 4. Project List.

Vendor Selection

Based on the organizations procurement policies it may require Vendor Analysis in order to select the best product at the best price. A Request for Proposal (RFP) should be submitted to a minimum of three vendors for each product selection. Starting with the top 3 vendors in the magic quadrant is best practice if budget allows. NDA's will need to be signed and agreed upon. Once the product selection is complete a proof of concept should be implemented in order to validate the vendor's responses. If the proof of concept works as planned then the project should proceed with the vendor selected product. If not, the 2nd place selection should be validated with yet another proof of concept before funding is committed.

Deployment Strategy

Once the RFP, vendor selection, and proof of concept have completed successfully the deployment plan should be developed and implemented. With changing technological solutions, subject matter expertise may not be available in-house. Acquiring technical expertise from the vendor could significantly reduce the amount of time and frustration with the deployment of the product. The vendor will also be aware of process and other changes that may be required in order to successfully deploy their solution.

DLP Deployment

Steering

To successfully deploy DLP processes, communications, and policies must be in order. A steering committee consisting of leadership needs to be established that approves new DLP policies. Members should consist of senior leadership, legal, HR, Information Security, Corporate Security, and the CISO. If the organization is conducting business in Europe consider Data Privacy Officer (DPO) should be considered as well.

This steering committee will also be responsible for the incident response process when an incident is triggered for investigation. These individuals are critical to the success of the overall process. Committee members must be conversant with and follow all legal and HR requirements in handling data and personnel as it is likely that an incident could lead to litigation or employee termination.

Staffing

The information security team will need additional staff to work with the business units on rule creation and addressing false positives through the implementation of exceptions. This will require significant effort in order to address the false positives until the rules are optimized.

Staff will also need to be trained on how and when to escalate an incident into an investigation status.

Policies

For the deployment, policies need to be refreshed and communicated to the end users so that they may familiarize themselves with changes in order to minimize any business disruption. Users will need to receive an explanation of the policies. This explanation should include how the policy affects them and what the consequences are for failing to adhere to them.

Technical Deployment

The overall network architecture will need to be reviewed from a technical perspective and placement of the new DLP infrastructure will have to be placed strategically in order to be effective. A review with the vendor is needed in order to verify the successful capture of data. Deployment of hardware and software will be required with the assistance of IT support. Once the deployment is complete, testing will need to validate that each component is working correctly.

Rule Creation

Each business unit should be contacted to identify resources to review existing business practices as they pertain to sensitive data. Identifying the most critical data first is best practice in order to safeguard the organization from critical data loss. This can be problematic as identifying the most critical data can be challenging.

Immediate focus should be on what can be accomplished short term and the subsequent implementation of a plan to address the unstructured data which will require scanning at a later stage of deployment. Focusing on 2-3 rules for each business unit in order to gain visibility into

the information data loss problem will ensure project manageability. A Review of regulatory requirements and out of the box templates is a best practice.

Rule Approval

Prior to rules implementation, the steering committee must approve them. This will ensure that the organization is following its code of conduct, legal, data privacy, and HR requirements before implementation. Without the appropriate approval, the collection of data could lead to legal action against the organization.

Rule Deployment

Once the approval is made the rules can be turned on and data collection can ensue. . During this time the incidents will be reviewed and monitored in order to identify false positives. This requires effort from the business unit and the information security team as modifications will be required and exceptions implemented to reduce the false positive count. Considerable effort may be required initially as the amount of data being produced may be significant.

Scanning

Scanning data repositories for sensitive data is the next step in a DLP employment once the initial rules have been implemented and are running efficiently. These repositories consist of file shares, SharePoint sites, and other databases. Businesses will have to produce the data locations and provide the required access in order to successfully scan these resources.

Scanning jobs will need to be deployed so that the information is properly identified. Once scanning is complete, this information can be used to identify sensitive data in other locations on the network. Depending on the product, it may be possible to quarantine the data so that it does not leave a specific location of the network.

Endpoint

Deploying the endpoint solution will require an agent on the clients, smartphones, and or tablets. Working with existing IT deployment methods will aid in successful deployment. Testing will be required before actions are enabled but this should not take very long as the actions are real time as they are initiated from the client.

This deployment will allow the information security team to implement rules which prevent data from being sent outside the company, copied to a USB drive, or copied from a file share whether the client is on the corporate network or not. This also can provide awareness to the end user as the ability to implement warnings based on possible human error or violations of policy is available and customizable.

DLP as a Control

Based on the many tools and capabilities DLP can reduce the threat of data loss due to human error, intellectual property, fraud, and it sabotage. If funding only permits one solution, this would be the recommended solution to implement. Layering of other products afterwards as funding permits in order to obtain a solid data loss prevention program is acceptable.

Integration

Integration with the other implementations for marking tools, secure email gateway, SIEM, and DRM will also need to be addressed. Policy can be implemented which take the decisions out of the hands of the end users. Integration with the secure email gateway rules can be created which identifies sensitive data that can be shared externally by forcing it through the email gateway in order to enable encryption. SIEM alerts can be triggered to warn the information security team of attempts to send critical data outside the company. DRM can be enabled on an attachment in order to properly protect the content before it leaves the company.

Marking tools can be utilized to tag and classify data so that DLP can easily identify the sensitive data and take action on it. All of these controls used in tandem can significantly reduce the threat of data loss within the organization.

Other Implementations

The marking tool, DRM, secure email gateway, and SIEM implementations are all basic implementations which need to be integrated within the DLP deployment. Technically these are not difficult implementations but all will require additional communications and changes to policies and procedures. Some will require end user training as they impact the user directly.

Marking Tool

The marking tool will be a change for the end users as it will require all documents be marked before they can be saved. This will require inclusion in the information security policy and point to the internal classification policy. This is the time to consider changes to the existing classification to align with the recommendations from Naomi Fine as discussed previously. End user education will be needed for the appropriate use of this tool. This control helps reduce the threat of intellectual property loss, human error, and possibly IT Fraud.

DRM

DRM will also require changes in policy as all sensitive data must have digital rights assigned to the files prior to sharing with business partners. This will enforce data security on the file once it leaves the organization. This also will require end user training so users will understand correct implementation of this solution. This control addresses the business partner threat as it not only limits what the client can do with the file but can also sets the file rights to expire after a predetermined time thus eliminating the business partner threat.

Secure Email Gateway

The secure email gateway will require policy changes as users will now have the ability to force email encryption. Policies should state the requirements as to under what circumstances email needs to be encrypted. Users will be required to undergo training on how to use this capability and when it is required. Once deployed, this solution can significantly reduce the threat of the business partner threat by encrypting the email prior to sending it.

SIEM

SIEM takes all log data and allows IT to correlate events and alerts based on significant findings. This implementation can significantly reduce the threat of insider sabotage and has the option of being deployed internally or outsourced as a managed service. This tool can alert based upon inappropriate admin access to systems and files. It can also work with the DLP deployment and alert based on attempts to send critical data outside the organization.

Control Gap Analysis and Hardening

Penetration testing will identify existing controls that need to be updated. Configuration modifications, software updates, and hardware updates may be required in order to address the gaps which were identified. This is an essential step which needs to be addressed as the assumption is made that once a control has been implemented the risk is alleviated. This is not the case, and requires constant attention. Hardening configurations and controls should be a part of the yearly program for data loss prevention.

Policy, Process, Procedures Review and Awareness Training

Based on the changes being made from a technical perspective, policies, processes, and procedures need to be reviewed and updated to reflect the current state. As mentioned in each of the technical implementations, there is a requirement to make updates based on the new

capability. Outside the new technology other policy statements need to be reviewed and updated periodically to keep pace with current threat vectors. New threats may have been introduced which require additional policy statements.

Awareness training is a critical element to the entire program. Users need to be informed and trained on all new requirements, features, and capabilities they now have to protect corporate data. Trained end users will have a major impact in protecting corporate data as they are the ones who are handling it on the front line. Training programs must be informative and be kept current. Making use of third party offerings such as SANS Securing the Human is one option in providing an in depth training program which can be modified to suit the needs of an organization without the expense of maintaining in-house expertise. Organizations need to understand that this is a critical component of data loss prevention as it is the user who has access that may be the biggest threat based on human error alone.

Risk Management

In order for a data loss prevention program to be effective it must work in conjunction with the risk management process. The risk management process is a cyclical task of assessing risk, evaluating existing controls, managing risk, and measuring effectiveness (Management Study Guide, 2012). Figure 5 from the Management Study Guide exemplifies the risk management process:

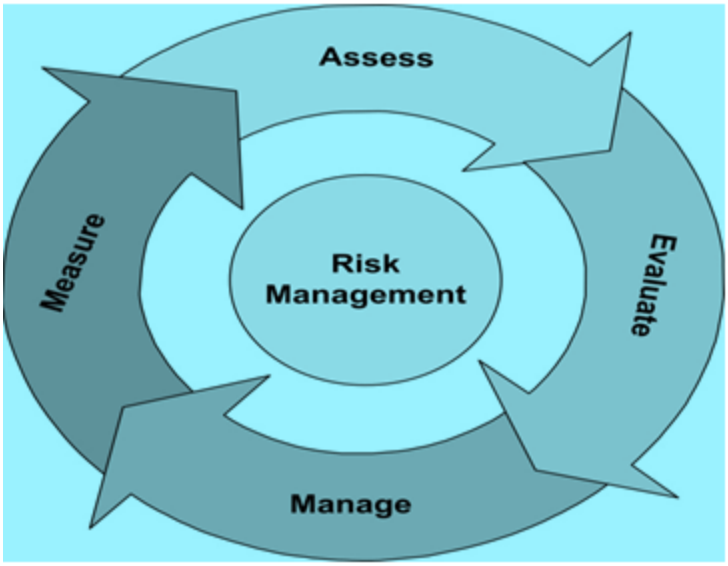

Figure 5. Risk Management Cycle.

By incorporating data loss prevention into the risk management cycle organizations can be assured that data loss controls will remain effective against the emerging threats. Each year changes to the threat vector are made pertaining to the insider threat; corporate espionage; foreign entities attempting to steal trade secrets; and competitors trying to gain competitive advantage through social engineering engagements and unethical practices.

Working in conjunction with IT/IRM, the data loss prevention program can take advantage of yearly penetration testing to validate controls, vulnerability assessments in order to identify possible weaknesses which may have resulted in a configuration change or failure of an update, and other threats that are new on the horizon such as the Advanced Persistent Threat (APT). New threats may require updates or new controls being implemented in order to reduce the risk to the organization. This is a mission critical element.

Chapter 6

Legal and Ethical Implications

When considering implementing a technology such as data loss prevention an organization may think that it is the right of the employer to implement systems and collect any data that it chooses s based on the legitimate concern of losing intellectual property. This assumption is incorrect and dangerous. There must be guidelines which are followed in order to ensure that the corporation is not protecting personal employee data. There is no legal stance for a corporation to take action without addressing privacy law and can open the company to the threat of litigation.

Companies wishing to conduct business in Europe must take into consideration the Safe Harbor Agreement which addresses the differences between the US and European privacy law (export.gov). This joint commission of the US Department of Commerce and the European commission provide the requirements for protecting the privacy rights of the various countries (export.gov). Becoming Safe Harbor compliant is best practice for organizations seeking to obtain trust in the countries they conduct business in.

Legal concerns arise based on various countries and even states which need to be taken into consideration. Germany "…is regarded as having the strictest data protection laws in the world. Germany privacy and data protection laws are vigorously enforced" (McAfee, 2012). The US states of Minnesota and California have both enacted data privacy legislation in order to protect the privacy rights of its residents.

Technical solutions such as DLP can be utilized to monitor email, documents, and SharePoint sites for privacy data. Based on the capability implemented, a company can scour the file servers and SharePoint repositories looking for data privacy issues. Once identified, the

organization can address threats appropriately. The right program in place will prevent data from being stored in its data storage repositories inappropriately without adequate protection. These actions can help enforce the requirements of the Safe Harbor Agreement.

Another mechanism that can be deployed through DLP is the prevention of users sending unprotected personal data through email or web transactions. This will keep data from being submitted electronically and avoid the risk of the data being accessed by individuals attempting to steal identities, bank account information, and social security numbers.

Technology with legal controls is the key to making use of applications such as Data Loss Prevention. The appropriate controls can enforce not only privacy law but also protect the organization from losing its intellectual property. This is a win-win from a corporate perspective when both concerns are addressed.

Ethics

Data loss prevention will involve the gathering of a significant amount of data. The use of the data collected must be limited to what it is intended and nothing more. From an ethical standpoint the organization must keep in mind its code of conduct, legal, regulatory, and other requirements to ensure that it is not collecting data inappropriately to avoid the threat of legal action.

Chapter 7

Conclusion

Data loss is a critical problem for every organization and can occur due to insider threat such as in the case of IT Sabotage, theft of intellectual property, fraud as well as external threats such as hactivism and social engineering, or simple human error. At this time, there is no solution available that offers the assurance of 100% protection from data loss. In order to reduce the immediate threat an organization must address the issues of people, policy, and technology together. The assumption that standalone technological solutions can offer adequate protection against the threat of data breach is dangerous and an unwitting invitation for a breach to occur.

Information Technology in conjunction with Legal, HR, Corporate Information Security, and senior leadership, should implement policies that can be enforced by technical solutions, processes and individuals to protect sensitive data. Without the commitment from the leadership team, this effort to protect data is meaningless.

Headlines every week showcase a new reported data breach. Competent leadership can minimize the risk of their company being next reported breach by putting people, policy and technology together. The motto for any prepared DLP program should be Data Breach: It's not an "IF"; it's a "When".

References

Capelli, D., Moore, A., & Trzeciak, R. (2012). The cert guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud). Upper Saddle River, NJ: Pearson Education, Inc.

Cisco. (n.d.). *Cisco asa 5500 series adaptive security appliances*. Retrieved from http://www.cisco.com/en/US/products/ps6120/index.html

Databreaches.net. (2011, December 14). *I can just picture it*. Retrieved from http://www.databreaches.net/?p=22173

Dealing with data security. (2012, June 22). *Top 6 data breaches for 2012, thus far*. Retrieved from http://datasecurityweekly.com/top-6-data-breaches-for-2012-thus-far/

Ernst, & Young. (2011, October). *Data loss prevention: keeping your sensitive data out of the public domain* [White Paper]. Retrieved from http://www.ey.com/Publication/vwLUAssets/Keeping_your_sensitive_data_out_of_the_public_domain/$FILE/Data_loss_prevention_Keeping_your_sensitive_data_out_of_the_public_domain.pdf

Export.gov. (2012). *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*. Retrieved from http://export.gov/safeharbor/

Fine, N. (2011). *Positively confidential*. Los Altos, CA: Reasonable Measures Publishing.

Gartner. (2012). *Gartner magic quadrant for secure email gateways, 2012*. Retrieved from http://www.proofpoint.com/id/gartner-email-security-magic-quadrant/index.php

Gartner. (August 10, 2011). *Magic quadrant for content-aware data loss prevention* (Research Note G00213871). Retrieved from http://www.gartner.com/technology/reprints.do?id=1-16XQWWD&ct=110810&st=sb

Gartner. (May 24, 2012). *Magic quadrant for secure web gateways* (Magic Quadrant for Secure Web Gateways 2012, p. 1). Retrieved from http://www.gartner.com/technology/reprints.do?id=1-1ANRDN9&ct=120525&st=sb

Gartner. (May 24, 2012). *Magic quadrant for security information and event management* (Magic Quadrant 2012). Retrieved from http://www.gartner.com/technology/reprints.do?id=1-1ATPEL3&ct=120608&st=sg

Grimes, R. (March 12, 2012). *Insider threat deep dive* (Deep Dive Series). Retrieved from http://www.infoworld.com/sites/infoworld.com/files/insiderthreat_nologo.pdf

Hajela, S. (2009, March 18). *Demystifying it governance*. Retrieved from https://www.cioindex.com/it_Governance/smid/1408/ArticleID/552.aspx

Hayes, M. (2011, September 28). Natural disasters and data loss! Message posted to http://businessblogs.co.nz/2011/09/natural-disasters-and-data-loss/

Management Study Guide. (2012). *Risk management - a basic understanding*. Retrieved from http://www.managementstudyguide.com/risk-management.htm

McAfee. (2012). *International privacy and data protection laws*. Retrieved from http://www.mcafee.com/us/regulations/international.aspx

McGann, J. (2012, July 6). *4 Crucial steps to manage data*. Retrieved from http://fcw.com/Articles/2012/07/15/COMMENT-Jim-McGann-data-strategies.aspx?Page=1

McMillan, R. (2008, July 15). *Update: it admin locks up san francisco's network*. Retrieved from http://www.computerworld.com/s/article/9110176/Update_IT_admin_locks_up_San_Francisco_s_network?taxonomyId=17&pageNumber=1

Nolo. (2012). *Nondisclosure Agreements*. Retrieved from http://www.nolo.com/legal-encyclopedia/nondisclosure-agreements-29630.html

Olavsrud, T. (2012, August 15). *How to secure data by addressing the human element* [Article]. Retrieved from http://www.cio.com/article/713753/How_to_Secure_Data_by_Addressing_the_Human_Element

Open security foundation. (2012). *Data loss statistics*. Retrieved from http://datalossdb.org/statistics?utf8=%E2%9C%93&timeframe=current_year

Ponemon Institute LLC. (2012). *2011 Cost of data breach study: united states* (2011 cost of data breach). Retrieved from http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf

Ponemon Institute LLC. (2012, July). *2012 Confidential documents at risk study* (Ponemon Institute Research Report). Retrieved from http://www.ciosummits.com/media/pdf/solution_spotlight/Ponemon%20White%20Paper%20FINAL.pdf

PriceWaterhouseCoopers. (January 25, 2007). *It governance in practice* (Insight from leading CIOs, p. 27). Retrieved from http://www.pwc.com/en_mt/mt/publications/assets/it-governance-in-practice-jan-2007.pdf

Privacy rights clearinghouse. (2012). *Chronology of data breaches*. Retrieved from http://www.privacyrights.org/data-breach/new

Rashid, F. (2011, March 1). *Hbgary federal ceo aaron barr quits due to anonymous attack* [Article]. Retrieved from http://www.eweek.com/c/a/Security/HBGary-Federal-CEO-Aaron-Barr-Quits-Due-to-Anonymous-Attack-325042/

Rashid, F. (2011, May 25). *It security & network security news & reviews: 10 biggest data breachs of 2011 so far* [Article]. Retrieved from http://www.eweek.com/c/a/Security/10-Biggest-Data-Breaches-of-2011-So-Far-175567/

Reuters. (2012, August 29). *Second lulzsec hacker arrested in u.s. in sony computer breach*. Retrieved from http://www.nydailynews.com/news/national/lulzsec-hacker-arrested-u-s-sony-computer-breach-article-1.1146923

The SANS Institute. (2011). *Understanding Encryption*. Retrieved from http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201107_en.pdf

SANS. (2012). *Critical control 17: data loss prevention*. Retrieved from http://www.sans.org/critical-security-controls/control.php?id=17

SANS. (2012). *Security awareness for the 21st century* [Brochure]. Retrieved from http://www.securingthehuman.org/media/resources/pdfs/security-awareness-brochure.pdf

Sniderman, Z. (2012, January 26). *Anonymous strikes: symantec says stop using pcanywhere*. Retrieved from http://mashable.com/2012/01/26/anonymous-symantec-pcanywhere/

Symantec. (2010). *Importance of corporate security policy*. Retrieved from http://securityresponse.symantec.com/avcenter/security/Content/security.articles/corp.security.policy.html

Symantec. (2010). *PGP Universal Gateway Email*. Retrieved from http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-pgp_universal_gateway_email_DS_21064412.en-us.pdf

Symantec. (2011). *Symantec data loss prevention for endpoint*. Retrieved from http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-dlp_for_endpoint_DS_21189146.en-us.pdf

Symantec. (2011). *Symantec data loss prevention for network*. Retrieved from http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-dlp_for_network_DS_21189691.en-us.pdf

Symantec. (2011). *Symantec data loss prevention for storage*. Retrieved from http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-dlp_for_storage_DS_21194670.en-us.pdf

Titus. (2012). *User driven classification for documents*. Retrieved from http://www.titus.com/software/document-classification/index.php

Verizon. (2012). *2012 Data breach investigations report* (Data breach investigations report). Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Watchdox. (2012). *Access, share and control enterprise files anywhere on any mobile device*. Retrieved from http://www2.watchdox.com/wp/site/enterprise-digital-rights-management-software/?pi_ad_id=12874215009&gclid=COuRwInll7ICFYFo4Aod61UAag

Watchdox. (2012). *Document-centric security*. Retrieved from http://www2.watchdox.com/products/technology/document-centric-security/

Websense. (2011, November 30). *Understanding the reasons behind data loss disasters* [White paper]. Retrieved from http://www.mwlsystems.co.uk/files/whitepaper-websense-understanding-and-avoiding-data-loss-uk.pdf

Zetter, K. (2011, August 26). *Researchers uncover rsa phishing attack, hiding in plain sight*. Retrieved from http://www.wired.com/threatlevel/2011/08/how-rsa-got-hacked/

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**