Raytheon | websense®

DATA LOSS RISK ASSESSMENT

websense
TRITON®

INTRODUCTION

The need to share information has never been greater as cross-organizational business processes become deeper and more complex. The movement of digital information, both within a business and across its increasingly porous boundaries to external individuals and organizations, carries more and more risk as regulations are tightened around data protection and personal privacy.

Organizations spend millions of dollars each year investing in business systems and processes to make information available to authorized employees and partners. And while these investments enable business to grow, they also pose significant risks to data loss and, by association, regulatory compliance, corporate governance, and brand and reputation, but most organizations do not know who all has access to confidential information, where all is the confidential information residing within the organization, which all channels and business processes allow confidential information to go outside the organization etc.

Consider the impact for an organization if its confidential data was inadvertently leaked over email, erroneously posted to a public Web site, or left unsecured on a laptop or USB drive. If it were intellectual property that was lost, consider the long term financial impact for an organization.

WEBSENSE DATA LOSS PREVENTION RISK ASSESSMENT – IDENTIFIES RISKS OF DATA LOSS.

Websense offers a 2-week Risk Assessment that allows organizations to qualify their risk of data loss. At the end of the engagement Websense would appraise the organizations on:

- What Channels and processes allow sensitive information to exit the corporate network?
- Whether sensitive information is exposed in open file shares and desktops?
- How much and what type of sensitive information is exiting the network?
- Who is transmitting confidential data and sensitive information outside the organization?
- What network protocols carry the most violations with respect to Data Loss?
- What regulations are being violated?

IDENTIFY YOUR DATA LOSS RISKS IN 2 WEEKS: A FOUR-STEP PROCESS

In a typical 2 week Risk Assessment exercise, our consultants using Websense DLP tools to create and implement data security policies to Identify and monitor confidential data wherever it is stored or used.

Websense Data Loss Prevention Discovery component quickly finds confidential data wherever it is stored including file servers, databases, document and email repositories, and web sites and the discovery task would be performed for a specific network within the organization during the assessment exercise and details scoping would be discussed prior to the Risk Assessment activity.

Websense Data Loss Prevention Monitoring module would be configured to monitor traffic exiting corporate network and this would inspects all network communications for confidential data sent in violation of data security policy designed during the assessment exercise.

Step 1: Risk Assessment Scope Freezing

During the assessment our consultants would work with your team to identify your top critical data for identified business units. During this exercise our consultants would work with you to freeze on what business units to target, determine high risk information, senders, and destinations; identify data types, file servers, and policies to be monitored; identify what regulations should the organization comply and the implications of non compliance to regulatory laws and review next steps in the Risk Assessment process. Also during this step the network architecture would be understood and the Plan for carrying out the assessment would be derived and submitted.

The typical participants from the organization during this step would typically include key decision makers and information owners, executive sponsors, project managers, security analysts, and network engineers.

Step 2: Policies Definition

Based on information gathered in the Scope Freezing step policies would be defined and the same would be configured based on the pre-defined policy templates available on the Websense Data Loss Prevention tool and through other data identification techniques that the tool provides.

Step 3: Discovery and Monitoring for two weeks

The next step is to discover sensitive information residing on a specific network, file servers etc and also to monitor confidential data leaving the organization network using Websense Data Loss Prevention tools. This step would clearly appraise your organization's current level of data risk, and what network protocol including email, instant message, FTP, web allow data leaks.

To effectively perform this step, Websense requires access to open file shares you wish to scan and access to your outbound-traffic via a port span or network tap. In most cases, the Websense Data Loss Prevention solution can be up and running within 30 minutes.

Step 4: Executive Presentation of Findings

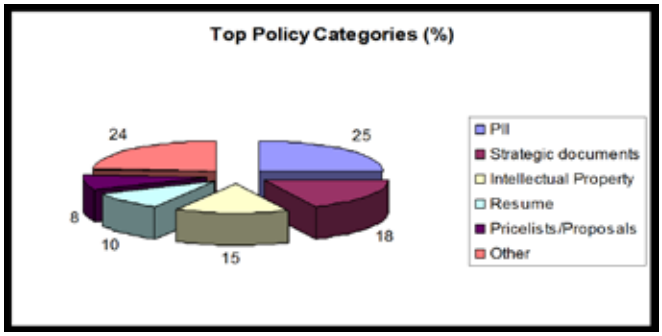
Following the discovery and monitoring phase, our team would analyze the incidents captured and identify the critical incidents and review the same with the team, once the right incidents and the nature of the same is determined, Our consultants would do a one hour executive level briefing to present and examine the results of the Risk Assessment exercise and discuss next steps. In addition, if required, Websense will build an overall business case for investing in Data Loss Prevention solutions with preliminary best practice commendations.

RISK ASSESSMENT DELIVERABLES

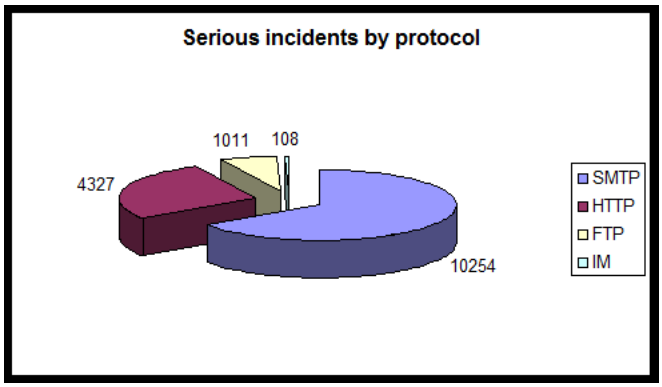
Once the exercise is performed a risk assessment report and a presentation would be submitted to you and some sample reports.

TOP POLICY CATEGORIES

Websense after performing the exercise would be able to identify the top policy violations as mentioned in the graph below. In the graph mentioned below, Personal information of customers was sent the most.

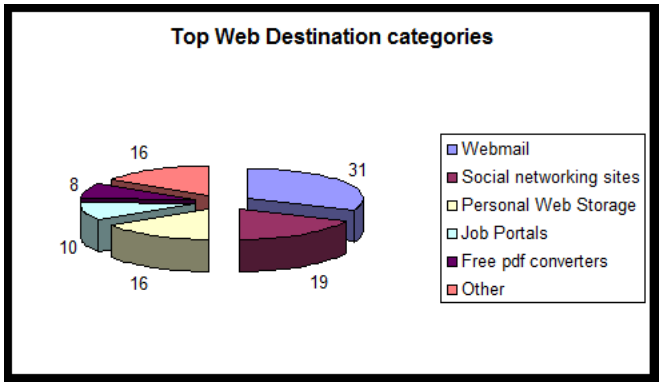


- Users sends out credit cards details of customers (in some incidents even more then 1000 CCN)
- 5 minutes after installing the system in the server room for POC , the customer found out that someone send out more the 10000 CCN – the reason for that was a malfunction printer



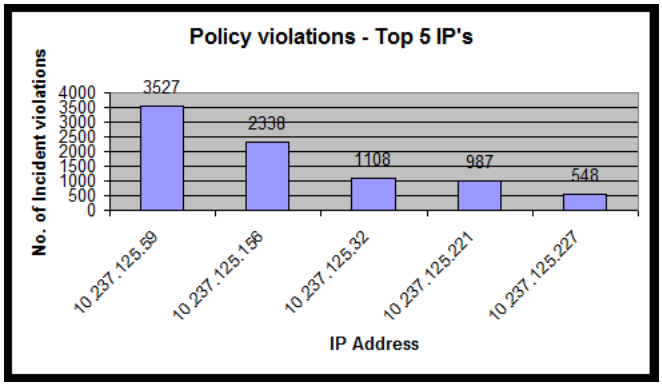
TOP VIOLATIONS BY PROTOCOL

Websense would inform the organization about the channel with which most amount of critical information gets leaked, we most of the times observe SMTP to be the protocol with which most information leaks.



We would submit the top web destination categories to which the information has gone, few examples of it are:

- Users used Google docs to edit and share financial documents like contracts, loans and more
- A VP sent out on his last day on work a document containing Intellectual property to his home account



We would submit the top users, user groups, departments who violate policies

Please find some critical incident details captured during the assessment from various verticals below.

VERTICAL	INCIDENTS
Finance	• A secretary had sent highly classified customer (American customer) information, as part of a document template • Users used Google docs to edit and share financial documents like contracts, loans and more • Users sends out credit cards details of customers (in some incidents even more then 1000 CCN) • Employee send out an excel sheet protected by password with financial details – the password attached in the body of the mail was "123456"
Telecom	• Customer DB view of a specific region was sent to an e-mail address in Russia (including names, address, ID and CCN) • 5 minutes after installing the system in the server room for POC , the customer found out that someone send out more the 10000 CCN – the reason for that was a malfunction printer • 1. Wrong workflow – customers CC# was distributed on an excel sheet without no encryption what so ever. • 2. A marketing user had intentionally leaked marketing information to the competition – the user was fired and the company filed a complaint • Marketing information was sent out by a user that was about to leave the company. The employee was caught and fired the same day • 15 wrong business processes were identified during the risk assessment and the customer admitted that he wasn't aware of these processes before the risk assessment.
IT/ITES	• Question Bank to select candidates was leaked to many email ID's through webmail. • Critical project specific information was sent out to many webmail ID's. • Source code information sent to many email ID's through webmail and SMTP
Insurance	• A VP sent out on his last day on work a document containing Intellectual property to his home account • 2006 business plan was sent by a VP to her son in order to shape the graphics and animation inside

VERTICAL	INCIDENTS
Manufacturing	• A confidential price list was sent out the SMTP channel • Senior functions within the organization are seeking for job from within the organization
Retail	• A log of cash registers system sent out to the supplier of the software found to contain enormous amount of customers credit cards

ABOUT WEBSENSE, INC.

Websense, Inc. is a global leader in protecting organizations from the latest cyber attacks and data theft. Websense TRITON comprehensive security solutions unify web security, email security, mobile security and data loss prevention (DLP) at the lowest total cost of ownership. Tens of thousands of enterprises rely on Websense TRITON security intelligence to stop advanced persistent threats, targeted attacks and evolving malware. Websense prevents data breaches, intellectual property theft and enforces security compliance and best practices. A global network of channel partners distributes scalable, unified appliance- and cloud-based Websense TRITON solutions.

Websense TRITON stops more threats. Visit www.websense.com/proveit to see proof.

TRITON STOPS MORE THREATS.
WE CAN PROVE IT.

websense TRITON®