



Professional Services

RISKADVISOR SERVICES ENGAGEMENT

FINAL REPORT



iTrust Security Ltd.
www.itrustsecurity.com



Table of Contents

Document Information	3
Executive Summary	4
Project Background and Objectives	4
Findings.....	4
Recommendations	5
Business and Technical Scope	6
Summary	6
Business Scope	6
Technical infrastructure Scope.....	6
Detailed Findings	8
Introduction	8
Technical Infrastructure Scan Results	8
Scanning Engagement Summary Table	8
Incidence Risk by Devices and File Shares	10
Summary Incidence Risk By Regulated Data Type	11
Incidence Risk by File Type	12
Business Process Discovery Results	13
Top Ten Offenders	13
Additional Workflow Findings, Analysis and Prioritization...	14
Recommendations	16
Appendix A: Supported File Format Types	17



DOCUMENT INFORMATION	
Prepared By:	<consultant name>
E-mail:	
Reviewed/Approved	
By:	<reviewer name>
Create Date:	10/19/07

Version History			
Version	Author	Date	Revision Notes

EXECUTIVE SUMMARY

PROJECT BACKGROUND AND OBJECTIVES

In response to Payment Card Industry (PCI) requirements around protection of sensitive cardholder information, <CUSTOMER> hired iTrust Security, the Security Division of EMC, to undertake a discovery of sensitive PCI data on a specified number of end-user laptops, desktops and corporate file shares, in order to gauge <CUSTOMER>'s exposure to the risk of undesirable disclosure of such data.

Additionally, <CUSTOMER> sought iTrust's assistance in identifying the business workflows that may have led to the placement of sensitive data on unauthorized devices and file shares, in order to determine if business workflow might be an effective remediation strategy. Finally, <CUSTOMER> requested that iTrust Security make specific recommendations for the management of PCI data - both to address immediate risks and to ensure that, going forward, <CUSTOMER>'s corporate security posture around management of PCI data would be optimally aligned with industry-standard best practices.

The current engagement was structured to address these objectives within the following scope for the data discovery scan:

- Geo-locations/business functions: New York (HR); Atlanta (IT); Chicago (Call Center)
- Devices: New York (~1000), Atlanta (~1500), Chicago (~2000)
- Corporate File Shares: N/A
- Data Types: PCI cardholder information and other Personally Identifiable Information (PII).

In addition to the automated scanning carried out for the devices and locations identified above, iTrust conducted interviews with individuals responsible for creation, retrieval, update and deletion of PCI and PII in order to develop an understanding of business workflow around handling of this sensitive data.

FINDINGS

Overall, the incidence of sensitive PCI data on non-authorized devices and file shares was found to be high, indicating significant vulnerabilities and risk around exposure of this data. Preliminary workflow analysis suggests that there are insufficient business workflow controls on processes relating to the creation, retrieval, update and deletion of PCI data inside the enterprise. The absence of such controls is likely a significant contributing cause of the high incidence of PCI data on non-authorized devices and file shares. [NOTE: The assessment of technical security controls was not in scope for this project.]

Among the detailed findings of the technical scan can be counted the following:

- Approximately 93% of the machines that were scanned had PCI/PII data
- A total of 50,400 files were found to have PCI/PII data
- Majority of the files that contained PCI/PII data were Microsoft Excel files
- Files with PCI data were equally spread across file shares and desktops
- None of the PCI/PII data was encrypted.

Additionally, the following workflows were found to play a significant role in the spread of regulated data to unauthorized devices and file shares:

- Data analysts in the HR department were found to be extracting employee data from Siebel and storing it in Excel spreadsheets on laptops and desktops, before sending it to ADP for payroll processing
- System developers were building applications to extend the online presence for <CUSTOMER>, were using “live” customer data for application development, test and QA, and were storing this data on their laptops and desktops
- Onsite third-party staff augmentation consultants working in the IT department stored “live” customer data to their laptops and routinely removed it from the premises at the end of each workday (and presumably at the end of their work contracts as well)
- Individuals in data management roles reported they were uncertain about company policies with respect to confidential data, and reported such policies were inconsistently enforced
- Gaps in policy and process controls causing data leakage around PCI and PII may indicate further vulnerability and risk around compromise of sensitive intellectual property data
- <CUSTOMER> has not yet carried out a systematic information risk assessment that would identify controls gaps in addition to the ones identified above.

RECOMMENDATIONS

In consideration of the <CUSTOMER>'s requirement for tactical recommendations that will address both the requirement to immediately address the risk from exposure of sensitive information, as well as more strategic recommendations that will, over time, bring <CUSTOMER>'s management of PCI data into line with industry best practices, iTrust recommends a two-phase remediation approach, as follows:

Phase I: Immediate Term

1. Notify highest incidence data leakage offenders via email containing a security awareness message and a request to purge files containing regulated data.
2. If <CUSTOMER> has current Acceptable Use Policy, then issue update that specifies all files sent to ADP should be password protected.
3. Identify files containing the highest incidence of regulated data and password protect the files that contain these data; priority should be files that are accessed by HR personnel.
4. Create a script to automatically clear the Temporary Internet Cache for all employees within the company; this should be deployed in the customer care organization first.
5. Review IT group development practices and issue guidelines for developers to ensure that “live” data is not used for application testing.
6. Initiate a limited business process re-engineering effort around those additional areas of workflow which create a high incidence of data leakage.

Phase II: Strategic Term

1. Initiate a comprehensive and systematic PCI Readiness Assessment and gap analysis around best practices business process (e.g., policies and procedures) and technology controls (e.g., authentication and access) for protection of sensitive PCI and PII data.
2. Depending on the outcome of this assessment, consider prioritizing and scheduling remediation recommendations into a single, project-based security improvement program.
3. Consider the purchase of a Tablus license in order to support cost-effective routine scanning of third-party contractor devices for sensitive PCI of IP data prior to contractor off-boarding at the conclusion of work contracts, as well as conduct periodic risk trending scans.

BUSINESS AND TECHNICAL SCOPE

SUMMARY

In consideration of the business objectives of the engagement, and based on partial assessments completed by <CUSTOMER> prior to the current engagement, <CUSTOMER> determined that the engagement scope should address what was expected to be a high risk business departments and associated technical infrastructure in geo-locations summarized in the chart below:

Geo-Locations	Scanned Network Sub-Nets	Business Function
New York	192.xxx.xxx.xxx	Human Resources (HR)
Atlanta	10.xxx.xxx.xxx	Information Technology (IT)
Chicago	172.xxx.xxx.xxx	Call Center (CC)
Chicago	10.xxx.xxx.xxx	Corporate Headquarters (CH)

These geo-locations encompassed business and technical infrastructure as described in the sections below.

BUSINESS SCOPE

As summarized above, business scope for the engagement encompassed three separate business functions, each in its own geo-location: HR, IT and CC. These business functions were chosen by <CUSTOMER> because each was identified as having access to sensitive PCI or PII data.

In-scope departmental roles, and in-scope workflows for each role, are summarized in the table below:

Data Type	Department	Role	Workflow
PII	HR	Analyst	Create/update employee record
PCI/PII	IT	SysAdmin	Archive customer account data
PCI	Business Unit	Fin. Operations	Review customer billing record
PII	Call Center	Analyst	Update customer trouble ticket

TECHNICAL INFRASTRUCTURE SCOPE

Technical infrastructure deployment comprised the following three major components:

- DLP DataCenter Enterprise Coordinator installed at the corporate headquarters in Chicago
- DLP DataCenter Site Coordinators installed in each of the major sub-nets, corresponding to the business departments identified above
- GridWorkers installed to scan file shares on each of the in-scope sub-nets.

All scans were managed from the corporate headquarters in Chicago, with a total of 4476 devices and file shares scanned. Excluded from the scan were printers, UNIX and other non-XP windows machines. The following diagram illustrates the technical infrastructure scanning scope:



Illustration 1: Scan Deployment Overview

DETAILED FINDINGS

INTRODUCTION

This section of the deliverable combines and summarizes the technical infrastructure scan and business process discovery findings; it is organized into two broad categories: (1) results of technical infrastructure discovery scan¹, and (2) results of business process workflow discovery.

The technical infrastructure scan discovery results are presented in a way that begins with a high-level summary across all scanned systems by location, followed by drill-down that indicates incidence risk² by file count, file type and incidence within files. Also included is a summary of the “top ten” offenders - individuals whose scanned machines contain the highest incidence of sensitive data. Each of these output presentations is described in detail, below.

The business workflow discovery and analysis section summarizes the following:

- results of validation checks on false positives and false negatives
- findings of data leakage causes as a result of workflow analysis
- list of top ten offenders for remediation.

TECHNICAL INFRASTRUCTURE SCAN RESULTS

Scanning Engagement Summary Table

The table below provides a summary of technical infrastructure device scan results for the entire engagement. Explanation of table columns is as follows:

- Location - The physical geo-location
- IP Range - The range of IP's scanned
- IP Total - The total number of possible IP's within that range
- Notes - Additional network structure description (e.g., main or intermediate distribution frame)
- Scanning status - In Process or Finished
- Total Systems with Data - Number of desktops or laptops where sensitive data was found
- Total Files with Data - Number of files containing sensitive data across all systems containing such data.

¹ These results are also presented in the DLP DataCenter product dashboard

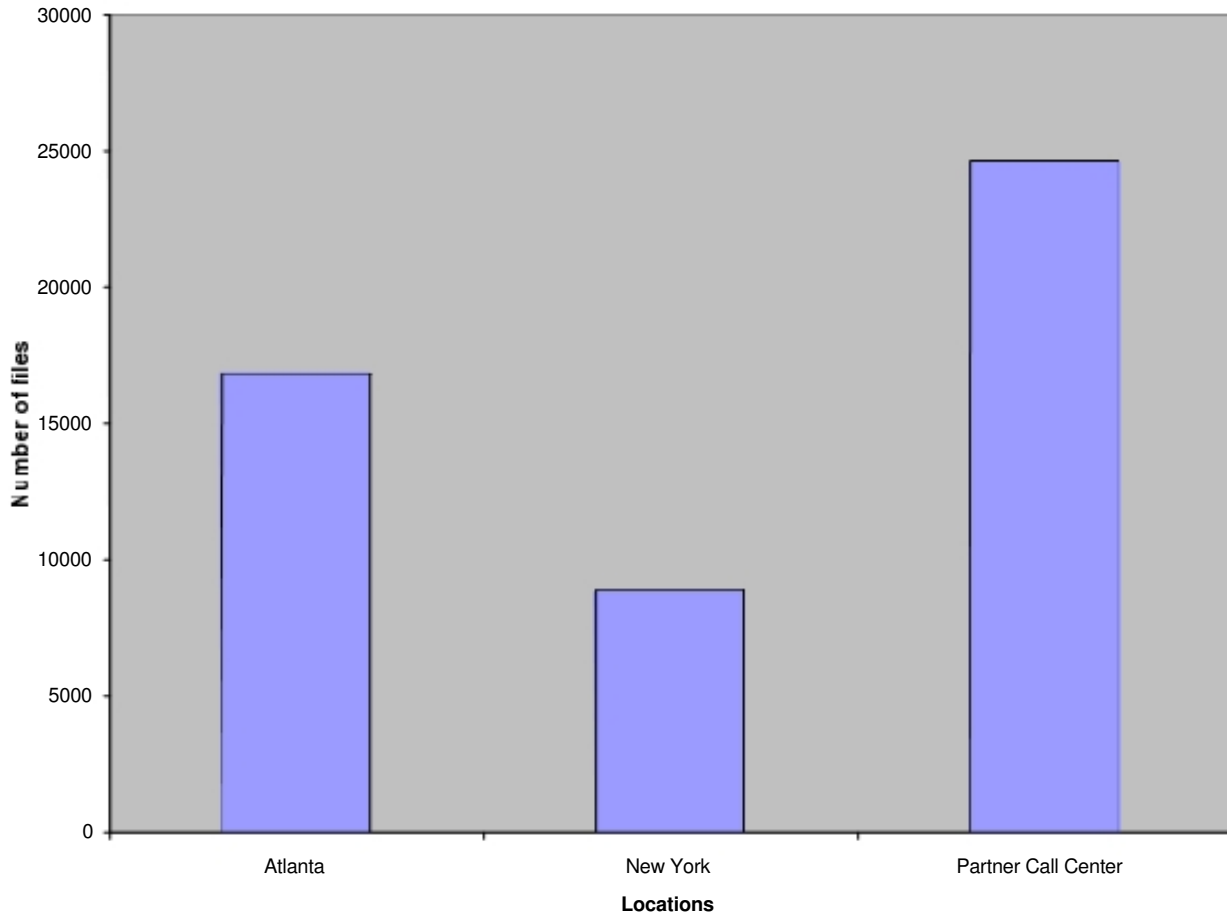
PCI/PII RiskAdvisor Scanning Engagement Summary

Location	IP Range	IP Total	Notes	Scanning Status	Total Systems Scanned	Total Systems w/Data	Total Files w/ Data
Atlanta	10.xxx.xxx.xxx	1024	KS1, IDF A	Finished	546	523	6276
Atlanta	10.xxx.xxx.xxx	1024	KS3, IDF B	Finished	82	59	708
Atlanta	10.xxx.xxx.xxx	256	Wireless	Finished	845	822	9864
Atlanta Site Total					1473	1404	16848
New York	192.xxx.xxx.xxx	1024	Wireless	Finished	87	64	768
New York	192.xxx.xxx.xxx	256	Vista 1st Floor	Finished	267	244	2928
New York	192.xxx.xxx.xxx	256	Vista 2nd Floor	Finished	457	434	5208
New York Site Total					811	742	8904
Chicago	172.xxx.xxx.xxx	1024	AT1, IDF C	Finished	56	33	396
Chicago	172.xxx.xxx.xxx	1024	AT3, IDF D	Finished	523	500	6000
Chicago	172.xxx.xxx.xxx	256	Wireless	Finished	987	964	11568
Chicago	172.xxx.xxx.xxx	1024	Wireless	Finished	42	19	228
Chicago	172.xxx.xxx.xxx	256	Horizon 1st Floor	Finished	557	534	6408
Chicago	172.xxx.xxx.xxx	256	Horizon 2nd Floor	Finished	27	4	48
Partner Call Center Site Total					2192	2054	24648
Total Number of Addresses		7680	Grand Total		4476	4200	50400

Among the important findings to be observed from this table are:

1. A very high percentage - 94% -- of systems in each geo-location contain sensitive data
2. The relatively large number of total files containing sensitive data, suggesting the need for additional business process discovery to understand the workflows which could have resulted in such a large incidence of file-based sensitive data.
3. The highest percentage of systems containing sensitive data (nearly 50%) are associated with the Call Center business function, suggesting this business department should be the high priority for remediation. The table below provides a graphical comparative summary of this statistic using data drawn from the Scanning Engagement Summary Table.

PCI/PII Files across Locations



Incidence Risk by Devices and File Shares

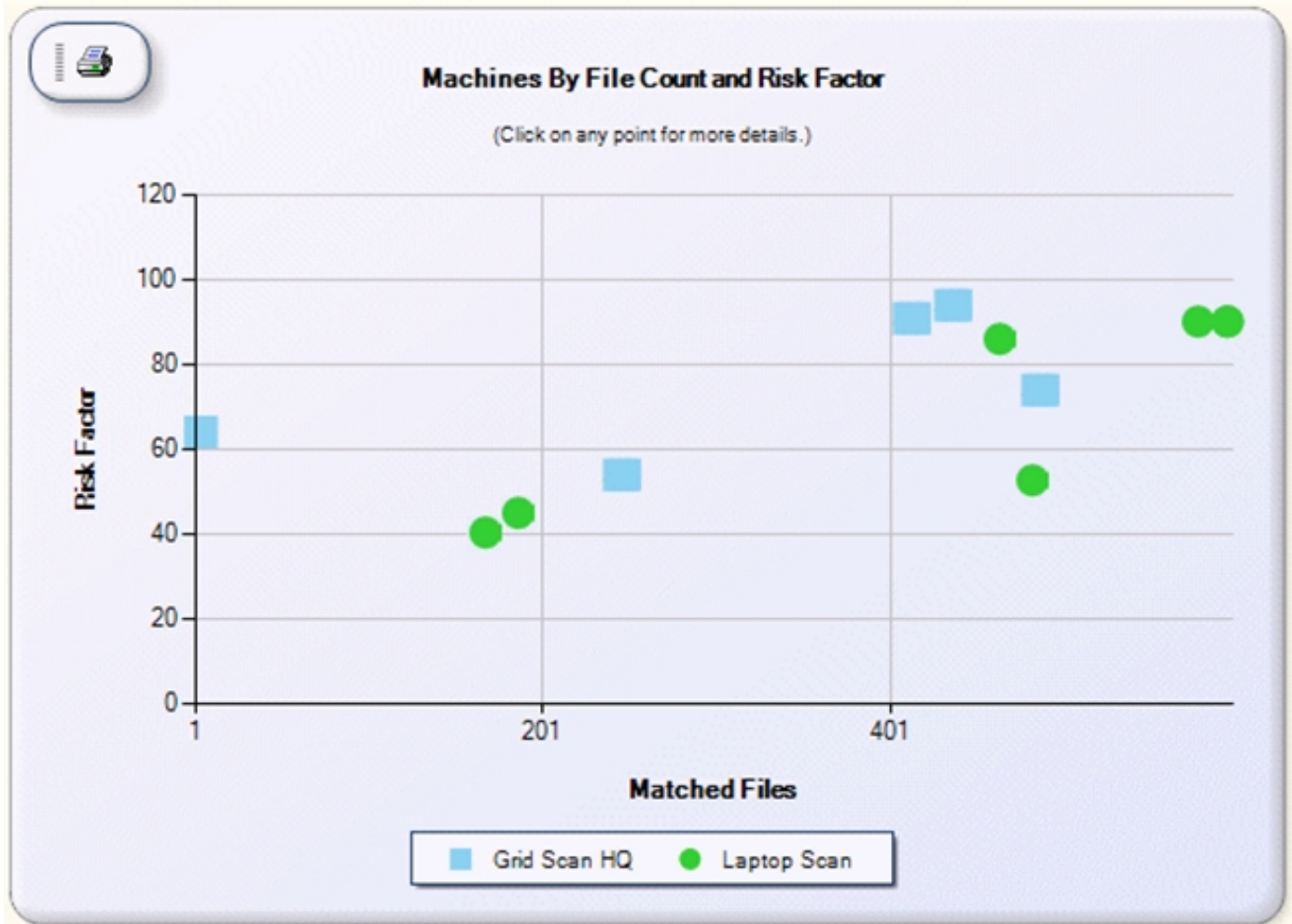
The graphic below identifies the set of highest risk devices and file shares, based on the incidence of sensitive data on these systems, using data drawn from the Scanning Engagement Summary Table³.

Explanation of the graphic components is as follows:

- Matched Files - Representation of an individual machine (laptop or file share) with the number of files with sensitive data
- Risk Factor - The risk factor (computed) based on the overall risk for that machine
- Grid Scan HQ - File shares at the company headquarters

³ Note this graphic is included for illustrative purposes only; file shares are not reflected in the Summary Engagement Table for this sample deliverable.

High risk factors indicate a high count of PCI/PII data detected within the files on a given device or share. These data suggest the need to prioritize the indicated devices and/or shares in deciding where to focus the analysis of business workflows in order to address this vulnerability.

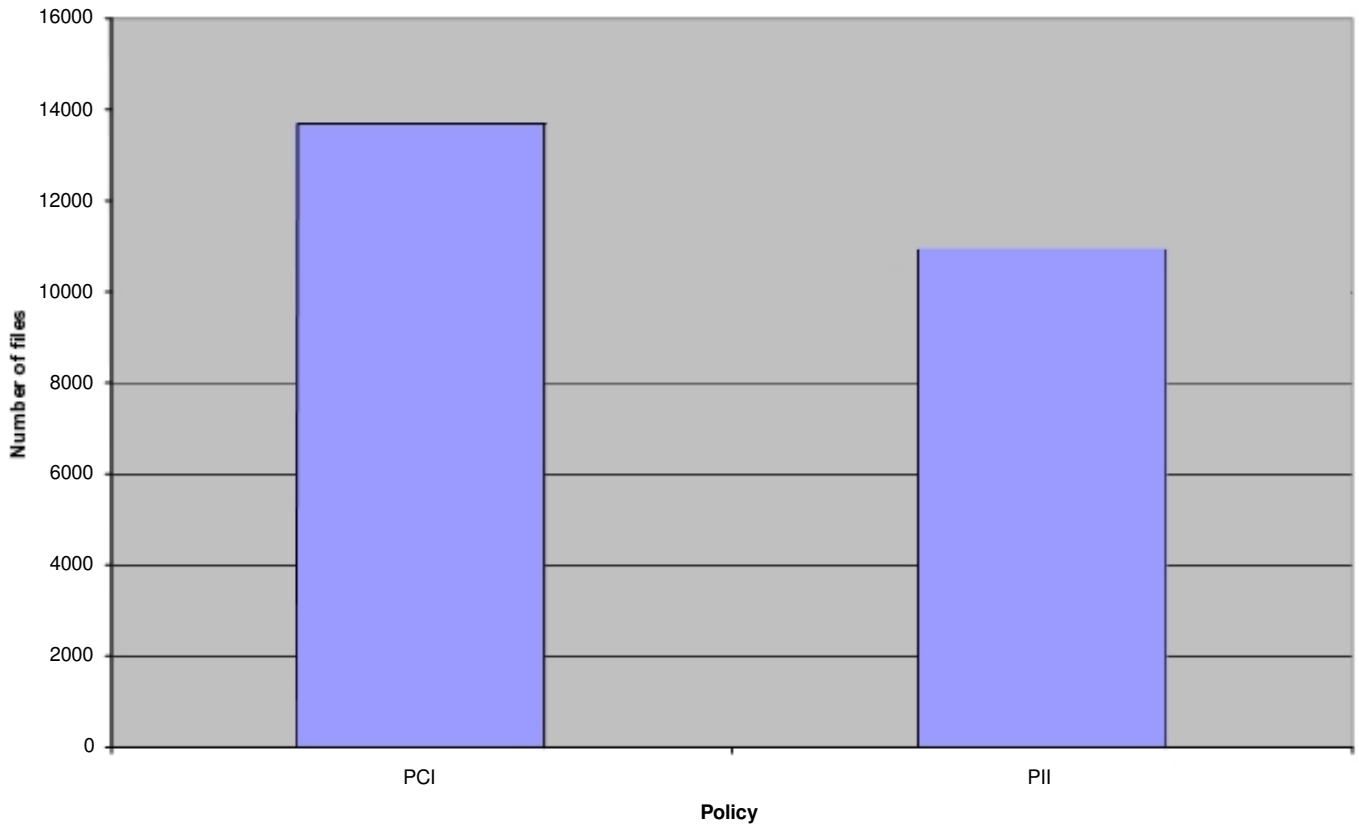


Summary Incidence Risk by Regulated Data Type

The graphic below provides a summary level display of the incidence of PCI versus PII data across the enterprise, using data drawn from the Scanning Engagement Summary Table⁴. The finding of rough parity in the total number of files containing PCI or PII violations suggests that workflows associated with both PCI and PII are to a roughly equal degree the cause of data leakage. By examining the specific workflows that are predominantly associated with specific data types (see below), it is possible to target remediation workflow-based remediation efforts.

⁴ File share incidence detail report is available in the DLP DataCenter results dashboard.

PCI/PII Violations across Enterprise



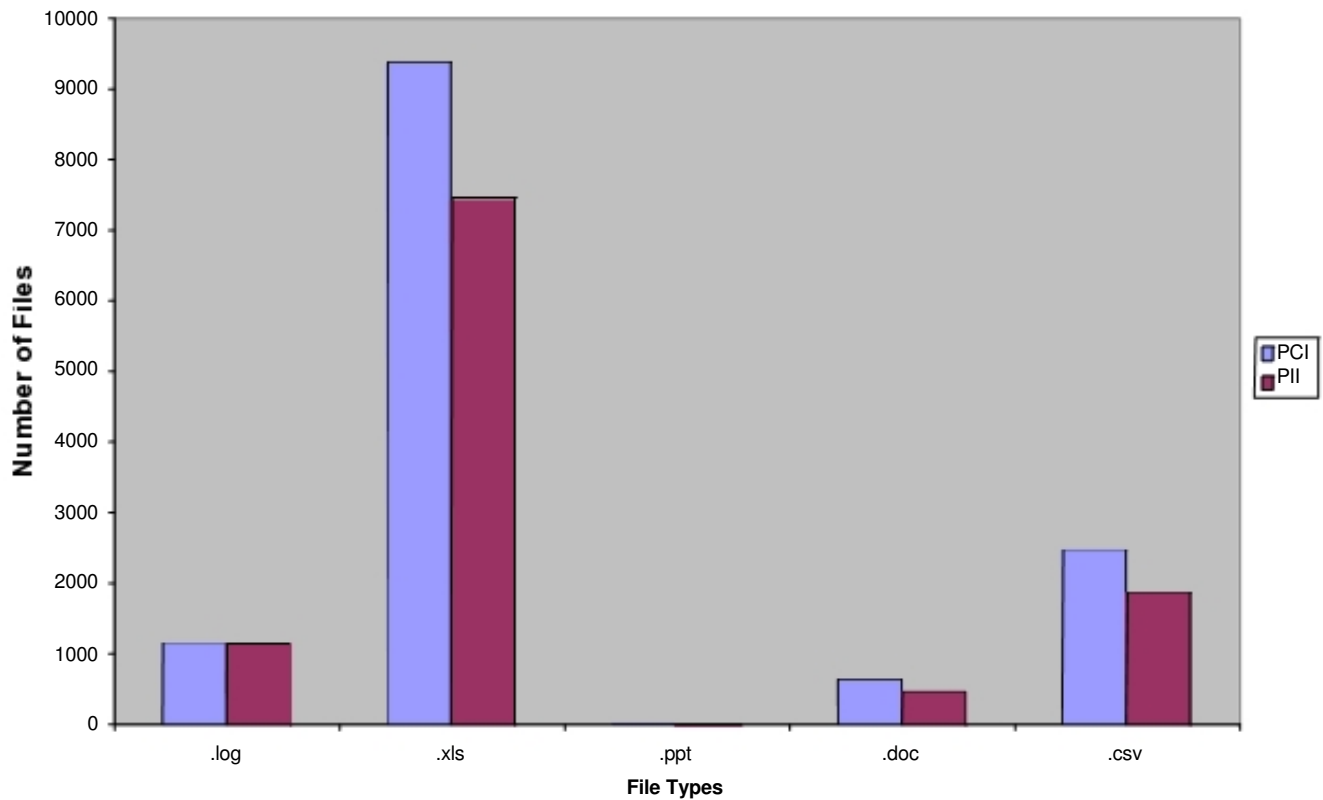
Incidence Risk by File Type

The graphic below provides a summary level display of the incidence of PCI versus PII data across the enterprise by common file types, using data drawn from the Scanning Engagement Summary Table⁵. The vertical axis, matched files, gauges the total number of files containing PCI or PII data. The graphic charts incidence for five file types drawn from the complete list of file types recognized by DLP DataCenter.⁶

The relatively large number of .xls and .cvs file types suggest areas for prioritizing business workflow discovery in order to determine which business functions are likely to generate these documents of this type and containing sensitive information.

⁵ File share incidence detail report is available in the DLP DataCenter results dashboard ⁶ See Appendix A for details.

PCI/PII Violations by File Type



BUSINESS PROCESS DISCOVERY RESULTS

Top Ten Offenders

The most direct method of associating workflow to levels of sensitive data on particular devices is to map those devices back to the identities of their owner/users. Profiles of the workflows associated with these owner users can then be developed, which provide important guidance on where business process remediation efforts should be focused.

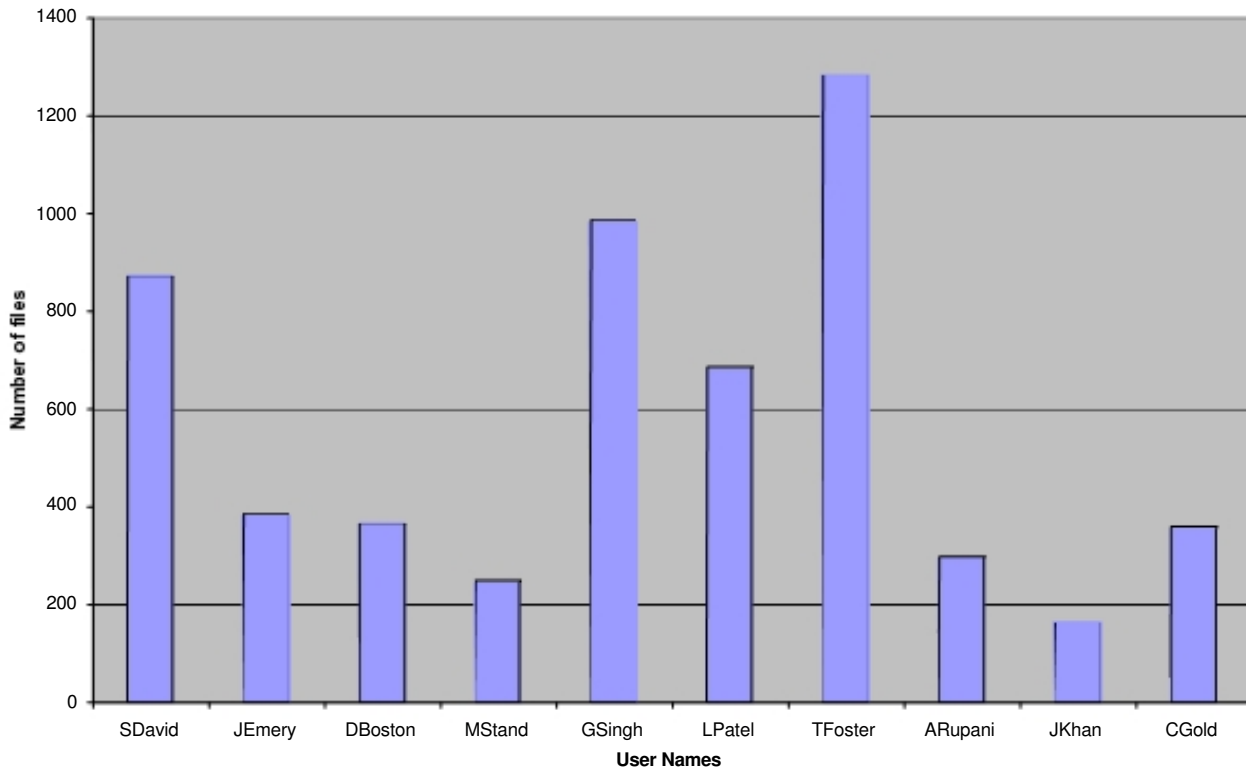
The graphic below reflects the results of this first-level workflow analysis, using data drawn from the Scanning Engagement Summary Table⁷. The vertical axis gauges the total number of files containing PCI or PII data; the horizontal axis reflects the results of mapping those laptops or desktops which were found to have to highest incidence of PCI/PII data to specific user/owner identities.

It is highly significant that all of the individuals identified below function as HR analysts, suggesting that <CUSTOMER> would be highly advised to focus any short-term business process workflow remediation efforts in this department. At the same time, however, it is important to note that top offenders constitute only 22% of the total number of files containing PCI/PII data, suggesting a widespread data leakage

⁷ File share incidence detail report is available in the DLP DataCenter results dashboard

problem throughout these business functions that can likely be effectively addressed only through a broader effort to understand root causes of PCI/PII data leakage.

Top Offenders



Additional Workflow Findings, Analysis and Prioritization

Beyond the analysis of top ten offenders summarized above, the preliminary workflow analysis took into consideration the following additional important findings from the technical scan results:

1. The relatively large number of files containing PCI/PII data (94% of total) suggests both a wide range of workflow activities and a high-volume of file access activities (create, retrieve, update or delete) daily activity; this was confirmed through interviews with a sample of individuals in each primary departmental role at each geo-location.
2. The finding of rough parity in the total number of files containing PCI or PII violations suggests that workflows associated with both PCI and PII are to a roughly equal degree the cause of data leakage.
3. File types containing the highest incidence of sensitive data are excel files (.xls) used for exporting data (primarily PII) out of HR applications, and .csv files containing sensitive data (both PCI and PII) exported for software testing purposes by the IT organization.
4. The largest number of files containing sensitive data is found in the Call Center. Follow-up workflow discovery by iTrust security indicates that the high incidence of files containing PCI data on Call Center systems files can be attributed to failure of Call Center analysts to clear the Web browser temporary cache, where this data was typically found according to scan results.

Because the scope of workflow discovery and for this engagement was not exhaustive, data leakage root cause analysis and remediation prioritization is difficult. More importantly, where there are many devices to be scanned, an exhaustive forensics that would map devices to specific identities is not practicable. An accurate diagnosis of exactly how business workflow results in leakage of sensitive data will typically require repeat scans carefully scheduled to yield further discovery around this organizational behavior.

Nevertheless, based on the above one-time technical scan and business process workflow findings, iTrust is prepared to draw the preliminary conclusion that a large percentage of <CUSTOMER>'s data leakage problem can be attributed to inadequate workflow controls within each of the three business departments/functions. This is supported by the finding that, although different departments handle different types of data (e.g., PII for HR and PCI for accounting), roughly equal incidences of the two sensitive data types were found throughout the enterprise.

Based on these findings, iTrust suggests that the highest priorities for remediation are workflow around PII data handlers in the HR department and software developers in the IT department, who are using live PII data to test applications. This suggestion is supported by the finding that the highest incidence of PCI/PII data leakage is found in .xls and .cvs file types, which are typically generated by HR analysts and software developers, respectively.

It should be noted that, while the Call Center has associated with it a large number of files with PII data, the fact that the total incidence of PII throughout the enterprise is proportionally lower than PCI suggests the incidence of PII data *per file* associated with the Call Center is relatively low, and thus the total risk associated with exposure of one or more Call Center files is lower than the risk of files originating within the HR and IT departments.

RECOMMENDATIONS

In response to regulatory compliance security requirements to remediate the risk of exposing regulated data, enterprises can undertake a range of actions. The best practices approach is typically programmatic: carrying out a broad and standards-based security vulnerability assessment, including a systematic data classification and inventory, followed by development of a risk prioritization and management strategy, and culminating in the definition of one or more project-level security vulnerability remediation initiatives. iTrust is the industry leader in providing services and products to enable such security improvement program development.

In consideration of the <CUSTOMER>'s requirement for tactical recommendations that will address both the requirement to immediately address the risk from exposure of sensitive information, as well as more strategic recommendations that will, over time, bring <CUSTOMER>'s management of PCI data into line with industry best practices, iTrust recommends a two-phase remediation approach, as follows:

Phase I: Immediate Term

1. Notify highest incidence data leakage offenders via email containing a security awareness message and a request to purge files containing regulated data.
2. If <CUSTOMER> has current Acceptable Use Policy, then issue update that specifies all files sent to ADP should be password protected.
3. Identify files containing the highest incidence of regulated data and password protect the files that contain these data; priority should be files that are accessed by HR personnel.
4. Create a script to automatically clear the Temporary Internet Cache for all employees within the company; this should be deployed in the Customer Care organization first.
5. Review IT group development practices and issue guidelines for developers to ensure that "live" data is not used for application testing.
6. Initiate a limited business process re-engineering effort around those additional areas of workflow which create a high incidence of data leakage; highest priority should be given to HR analyst workflow that touches PII data.

Phase II: Strategic Term

1. Initiate a comprehensive and systematic PCI Readiness Assessment and gap analysis around best practices business process (e.g., policies and procedures) and technology controls (e.g., authentication and access) for protection of sensitive PCI and PII data.
2. Depending on the outcome of this assessment, consider prioritizing and scheduling remediation recommendations into a single, project-based security improvement program.
3. Consider the purchase of a Tablus license in order to support cost-effective periodic risk trending scans, in order to measure the effectiveness of tactical risk remediation steps in addressing the problem of sensitive data leakage.

APPENDIX A: SUPPORTED FILE FORMAT TYPES

Class	File Format	Version Info	Extension
Archive	BinHex	Na	HQX
	GZIP	2	GZ
	Java Archive	Na	JAR
	PKZIP	through 6.2g	ZIP
	WinZip	through 9.0	ZIP
	Tape Archive	Na	TAR
	UNIX Compress	Na	Z
	UUEncoding	2.1	UUE
	RAR Archive format		RAR
Computer-Aided Design	AutoCAD Drawing	R13, R14, 2000, 2004	DWG
	AutoCAD Drawing Exchange	R13, R14, 2000, 2004	DXF
	Microsoft Visio	5, 2000, 2003	VSD
Mail Formats	Microsoft Outlook	97, 2000, 2002, 2003	MSG
	Microsoft Outlook Express	Windows 6, Macintosh 5	EML
	Microsoft Outlook Personal Folders	97, 2000, 2002, 2003	PST
	Text Mail (MIME)	Na	Various
Display Format	Adobe Portable Document Format	1.1-1.6	PDF
Presentation Graphics	Applix Presents	4.0, 4.2-4.4	AG
	Corel Presentations	7,9,10,11, 2000	SHW
	Lotus Freelance 2	2	PRE
	Lotus Freelance 96+	96,97,98, R9, 9.8	PRE
	Microsoft Powerpoint PC	4	PPT
	Microsoft Powerpoint 95	95	PPT
	Microsoft Powerpoint 97+	97, 2000, 2002, 2003	PPT
	Microsoft Powerpoint Mac	98	PPT
	Micromedia Flash		SWF
Graphics	Enhanced Windows Metafile	Na	EMF
	Lotus PIC	Na	PIC
	Windows Metafile	3	WMF
Spreadsheet	Applix Spreadsheets	4.2,4.3,4.4	AS
	Lotus 1-2.3 Charts	2,3,4,5	123

	Comma Separated Value	Na	CSV
	Microsoft Excel	2,2,3,4,5,96,97,2000,XP,2003	XLS
	Microsoft Excel Charts	2,3,4,5,6,7	XLS
	Microsoft Excel Macintosh	98	XLS
	Lotus 1-2-3 V2-5	2,3,4,5	WK4
	Lotus 1-2-3 V96+	96,97,R9, 9.8	123
	Micrsoft Works Spreadsheet	1,2,3,4	S30,S40
	Corel Quattro Pro	5,6,7,8	QPW, WB3
Text and Markup	ANSI	Na	TXT
	ASCII	Na	TXT
	HTML	3, 4	HTM
	Rich Text Format	1.0-1.7	RTF
	Word Pad	through 2003	RTF
	Unicode Text	3,4	TXT
	Open Office	1, 1.1	Various
	Star Office	6, 7	Various
	Microsoft Excel Windows XML	2003	XML
	Microsoft Word Windows XML	2003	XML
	Microsoft Visio XML	2003	XML
	XHTML	1	HTM
	XML	1	XML
Word Processing	Adobe Maker Interchange Format	5.0, 5.5, 6,7	MIF
	Applix Words	3.11, 4.2, 4.3, 4.4, 4,41, 4.2, 4.4	AW
	IBM DCA / RFT	vSC23-0758.1	DC
	Display Write	4.0	IP
	Folio Flat File	3.1	FFF
	Fujitsu Oasys	7	OA2
	JustSystems Ichitaro	8,9,10,12	JTD
	Lotus AMI Pro	2, 3	SAM
	Lotus AMI Prof. Write Plus	2.1	AMI
	Lotus Word Pro	96, 97, R9	LWP
	Microsoft Word PC	4,5,5,5,6	DOC
	Microsoft Word V1-2	1.0, 2.0	DOC
	Microsoft Word V6-95	6,7,8,95	DOC
	Microsoft Word 97+	97, 2000, 2002, 2003	DOC
	Microsoft Word Macintosh	4,5,6,98	DOC
	Microsoft Works V1-4	1,2,3,4	WPS
	Microsoft Works 6+	6, 2000	WPS
	Word Perfect Macintosh	1.02, 2.0, 2.1, 2.2, 3.0, 3.1	WPS
	Word Perfect Windows V5	5, 5.1	WPS
	Word Perfect Linux	6, 8.1	WPS
	Word Perfect Windows V6+	6,7,8,10,11	WPD
	Haansoft Hangul	97	HWP
	Lotus SmartMaster (Win x86 only)	96, 97	MWP
	Microsoft Windows Write	1,2,3	WRI
	XYWrite	4.12	XY4



Databases	Microsoft Access	95, 97, 2000, 2003	MDB
-----------	------------------	--------------------	-----