



## Unsecured Personal Private Data Audit Report

**Customer:** COMPANYX  
**Date:** XX-YYY-2006 to XX-YYY-2006  
**Audit performed at:** COMPANY SITE  
**Report date:** XX YYYYYYY 2006

### **Disclaimer**

PixAlert does not guarantee that the data presented are the only data of a personal nature on the Company network at the time of scanning. PixAlert's auditing tool is not a forensic tool. It is designed to help organisations identify the presence of unsecured personal data on company computers. Opinions presented are based on the experience of PixAlert and its experienced consultants in this area. Clients are advised to seek independent legal advice to verify compliance and application of various employments, civil and criminal legislation.

## EXECUTIVE SUMMARY

On XX<sup>th</sup> YYYYYYYY 2006 through XX<sup>th</sup> YYYYYYYY 2006 PixAlert conducted a Privacy Audit on the network of COMPANYX. A PixAlert Privacy Audit provides companies with the visibility that they need to quantify the risk caused by unsecured personal digital information such as credit card numbers, social security numbers and other unsecured personal information in the workplace. It helps address legal and corporate obligations and provides valuable data on exposure level, sources of vulnerability and volume of unsecured data.

During the Audit PixAlert's Privacy Auditor software was used to analyse:

- 🔴 **PCs** – An analysis of desktops and laptops for unsecured personal content;
- 🔴 **Email** – Scans of email folders and exchange server mailboxes for unsecured personal information and tracks distribution inside and outside of the organisation;
- 🔴 **File Servers** – Scans user accounts on servers.

Looking for:

- 🔴 **Credit Card Numbers**
- 🔴 **Social Security Numbers** and related data
- 🔴 **Health Insurance Numbers** and related medical data
- 🔴 **Other Personal content** – such as Driving Licence Number, Insurance, passport data etc.

<b>Number of target shares scanned</b>	696	<b>Number of credit card numbers found</b>	15,773
<b>Amount of Data Scanned</b>	1,395 Gb	<b>Social Security Numbers found</b>	2,364
<b>Number of files scanned</b>	23,466,655	<b>Health insurance numbers found</b>	1,766
		<b>Other personal content found</b>	3,245

In addition to the 15,773 credit card numbers which were found, 3245 other types of personal data were found including driving licence numbers, mortgage details, and national identity card numbers and passport numbers A record of the location of all these personal data is available.

Unsecured personal information was mailed to sixty three (63) outside companies, sent using a COMPANYX corporate email address.

The above findings indicate that unsecured personal information is:

- 🔴 **widespread** within the company
- 🔴 **current** and ongoing
- 🔴 **not confined** within the company but involves external parties
- 🔴 **common** on desktop and laptop PCs
- 🔴 **common** on servers
- 🔴 **common** on email

### Risks

- 🔴 **Email vulnerability** High
- 🔴 **Internet vulnerability** Low
- 🔴 **Vulnerability via other routes** (e.g. USB) High
- 🔴 **Risk of reputational exposure** High

### Desktop / Laptop PCs

A common risk centre is Desktop and Laptop PCs with 24% of all unsecured personal information found coming from this source.

The majority of data found on desktops were contained in email files located on the PC (36%). Thirty percent (30%) of files containing unsecured personal data had been deliberately saved to disk, presumably for later use. Twenty four percent (24%) of files containing credit card data were sourced from the internet. Nearly 40% of files found containing personal information were created in 2006 indicating a current and ongoing compliance issue.

Desktops	
Number of Desktops scanned	103
Number of files holding unsecured personal data	376
Percentage of desktops affected	31.1%

### Servers

Servers	
Number of server accounts scanned	125
Number of files containing personal information	1,166
Percentage of server accounts affected	25.6%

By far the largest area of unsecured personal information abuse was found on file servers probably due to the fact that desktop computers are backed up automatically to the servers. Most of the data found on server shares were held in email files (93.6%). Fifty four percent (54%) of data found on file servers were created in 2006 indicating current and ongoing IT security issue.

### Email Servers

While email servers contained relatively few instances of unsecured personal information, email folders found on desktop PCs and Servers held a significant number of such files. A considerable number of emails containing unsecured personal were distributed to an outside 3<sup>rd</sup> party using a COMPANYX.com email account, a few of whom are listed in the table on the right.

In total (including Desktops, Servers and Microsoft Exchange Email accounts) 1251 illicit files containing personal information were found on email (79.3% of all data files discovered).

Email Servers	
Number of email server accounts scanned	122
Number of files added to report	25
Percentage of email server accounts affected	9 %
Inbound Emails	48.7 %
Outbound Emails	19.6 %
Internal Distribution	31.7 %
<b>3<sup>rd</sup> parties receiving unsecured personal information from COMPANYX include</b>	

## AUDITOR'S SUMMARY

### Auditor's Conclusions

- ▶ Unsecured Personal information is widespread and ongoing within COMPANYYX's site and constitutes a significant IT risk to COMPANYYX.
- ▶ The highest risk source of unsecured personal data is in Email;
- ▶ External distribution is common;
- ▶ Unsecured personal data have been sent, using a COMPANYYX corporate email address, to private sector organisations (suppliers, customers and competitors), public sector (central and regional government), universities and schools;
- ▶ Internal distribution is common and not contained to the COMPANY SITE COMPANYYX site;

### Scan Data

Overall the percentage of target shares which contained unsecured personal data was 21.5%.

During the scan the PixAlert Privacy Auditor software achieved a false positive rate of 0.22% meaning that out of the 23.5million files encountered 0.22% of the files analysed were incorrectly identified as personal data by the software. False positive data are not categorised by the auditor.

**Benchmark** - The average number of files containing personal data per share for the site was 2.3 compared with a UK average of 1.4. This indicates that more data were found per person than normal.

**Benchmark** - The average number of personal data per gigabyte for the site was 1.1 compared with a UK average of 2.47. Thus the data was more widely spread out.

**Benchmark** - 50.48% of personal data found on the site were created in 2006 compared with a UK average of 50.54%. This site is on a par with most other organisations audited.

### Source Data

The majority of data discovered during the audit were found in email. This is highly unusual and poses a significant risk to the organisation. Emails were found to have been received from outside accounts, sent internally and, more worryingly, sent externally.

A large number of personal data files were found in Microsoft Office documents, which are commonly emailed internally and externally and pose a high risk.

**Benchmark** - 79.3% of personal data were found in email compared with a UK average of 22.9%. This is a significant IT and compliance risk to the organisation.

**Benchmark** - Office documents containing unsecured personal data were found to hold an average 7.0 credit card numbers per document compared with a UK average of 0.8 credit card numbers per document. Thus office documents found during the audit held more numbers than the norm.

**Benchmark** - 59% of shares audited contained unsecured personal data held in Microsoft Office documents compared with a UK average of 21%. In the COMPANYYX COMPANY SITE site, distribution of unsecured personal data using Microsoft Office documents appears to be commonplace.

## Distribution

The same data found in multiple locations is an indication of multiple users sharing unsecured personal data. During the audit there appeared to be a larger number of 'repeat data' found than normal.

As discussed above, the extent of unsecured personal data discovered in email folders was much higher than the norm and is indication of widespread abuse. 51.3% of emails involved external or internal distribution indicating unhampered data distribution.

**Benchmark** - 18.76% of the shares audited contained data found on one or more other shares, compared with a UK average of 3.21%. This is indication of a widespread compliance risk.

**Benchmark** - 79.3% of files were found in email compared with a UK average of 22.9%. This is a significant IT and reputational risk to the organisation.

## Other file types

26.33 Gigabytes of Movie and Audio files were found, a large part was found on file servers.

As well as a large number data files found in Microsoft Outlook (.PST) file, PixAlert Privacy Auditor found a number personal data files in Lotus Notes files (.NSF).

## TOP 25 LOCATIONS CONTAINING UNSECURED PERSONAL INFORMATION

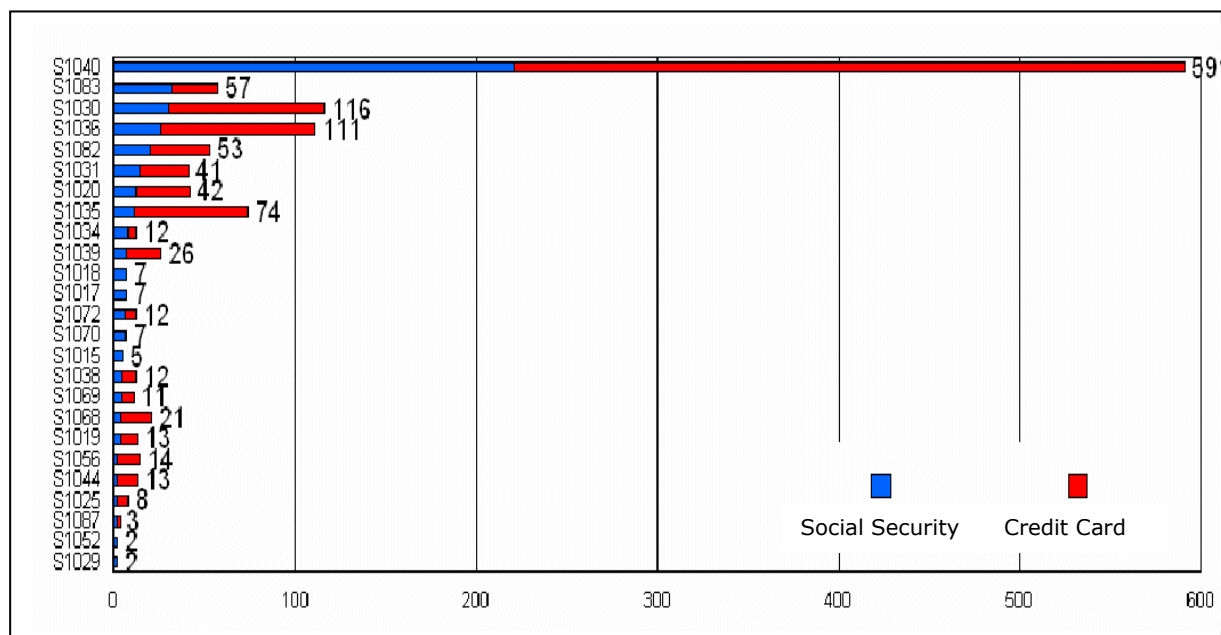


Figure 1: Top 25 Locations

### UNSECURED PERSONAL INFORMATION SOURCE

Unsecured personal data found were identified as having the following sources:

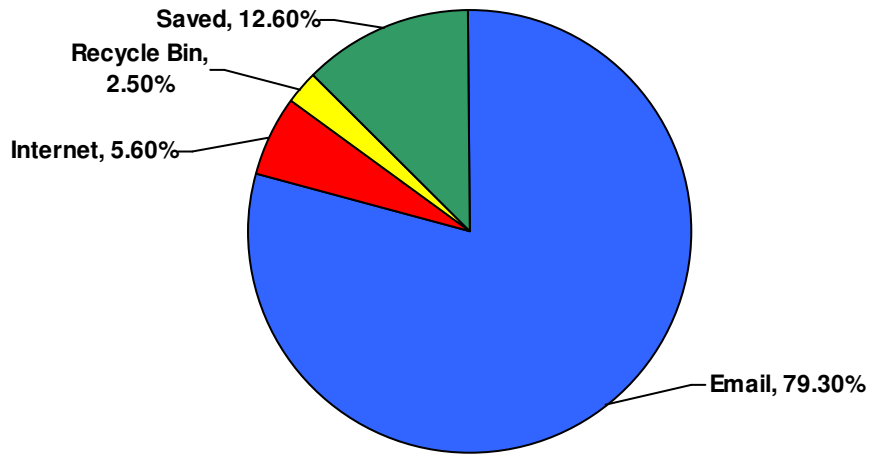


Figure 2: Data Source Analysis

### UNSECURED PERSONAL DATA TYPE ANALYSIS

	%	Credit Card	Social Security	Other	Total
Email	79.3%	354	895	2	1251
Internet	5.6%	17	72	0	89
Recycle Bin	2.5	23	16	0	39
Saved	12.6%	50	148	0	198
<b>Total</b>	<b>100%</b>	<b>444</b>	<b>1131</b>	<b>2</b>	<b>1577</b>

### SHARES CONTAINING UNSECURED PERSONAL CONTENT

