

# Critical Data Auditor

## Detection of unsecured, sensitive data



*"Information is the world's new currency. It must be guarded to protect against unauthorized disclosure, loss, or theft"*  
- IDC Study, 2008

*Before you can protect it, first you must find it" - PixAlert, 2008*

### What is Critical Data Auditor?

Data protection is now a critical corporate governance issue in the boardroom. Recent high profile data leakage events have damaged reputations while rising legislative and standards requirements create imperatives for action in this area.

Data Leakage Prevention (DLP) programs can help to secure critical and sensitive data, but firstly you must locate & identify the information you need to protect. Critical Data Auditor™ by PixAlert is scanning software to rapidly locate critical information and discover risk on company networks.

### Why Use it?

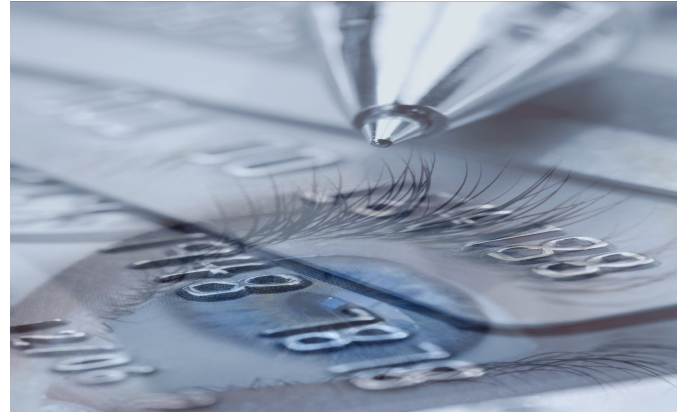
PixAlert's Critical Data Auditor is used to:

- satisfy legislation-based requirements;
- ensure compliance with policies & standards;
- conduct internal investigations;
- meet critical business or operational needs;
- perform audit & risk assessments.

### Typical Applications

PixAlert's Critical Data Auditor is used to:

- find & protect Intellectual Property;
- satisfy Freedom of Information requests, Competition Authority investigations, e-discovery orders and HR processes;
- conduct Due Diligence prior to acquisitions;
- check for confidentiality during 'quiet periods';
- check compliance with Data Retention, Data Protection Acts and other legislation;
- identify requirements for data archiving and data leakage prevention programs
- discover relevant data in criminal or civil investigations;
- Investigate for inappropriate or illegal use of I.T. resources;
- Identify critical data for back-up or encryption.



### Key Features

- **No impact** - on users or business critical systems;
- **No software installed** - on scan targets;
- **Scans data at rest** - which has been left unprotected on the file system;
- **Network Coverage** - detects critical information on PCs, File Servers and Corporate Email Servers;
- **File coverage** - no other software scans as many file types including Microsoft® Office, PDF, Email and Zip files;
- **Comprehensive reports** - provides management with up-to-date vulnerability assessment;
- **Identifies vulnerabilities** - in business practice and procedures and addresses them.

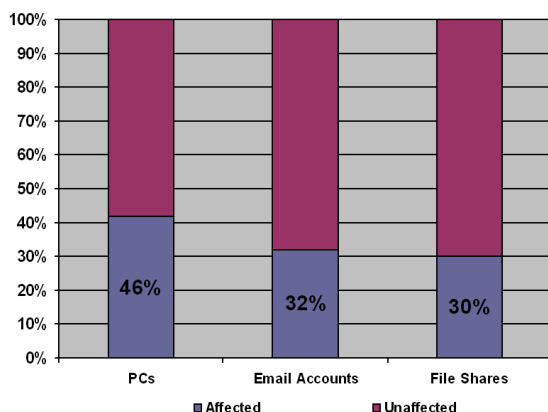
### Who should use it?

- Companies in regulated industries;
- Government Departments & public sector bodies;
- companies subject to PCI Security Standards Council regulation;
- companies compliant or certified for standards such as ISO 27000;
- Law firms, Auditors and professional services bodies;
- Regulatory authorities.

# PixAlert Critical Data Auditor

## PixAlert's Data Discovery Audit Findings 2007

### IT RESOURCES CONTAINING UNSECURED SENSITIVE DATA



*Identity Theft costs the UK economy £1.7billion*

*Home Office Identity Fraud Steering Committee, 2007*

Critical Data Auditor can aid compliance with standards, such as:

- Sarbanes Oxley Act;
- Basel II;
- EU data retention directive;
- UK Data Protection Act;
- EU Markets in Financial Instruments Directive;
- Payment Card Industry Standard (PCI);
- EU Audit and Privacy Directives;
- ISO 27001 information security standard;
- SB-1386: Security Breach Information Act;
- Gramm-Leach-Bliley Financial Services Modernization Act.

*"as much as 60% of corporate data resides unprotected on PC desktops and laptops."*

*IDC analyst*

*"The average cost for compromised data grew to £101 per record, up 43% since 2005"*

*The Ponemon Institute*

## **What does it look for?**

PixAlert Critical Data Auditor can be used to search for both structured data patterns (such as credit card numbers, social security numbers and passport data) and occurrences of unstructured search terms (such as a company or product name, a specific social security number or address etc.)

Search types can be combined, for example Critical Data Auditor may be tasked to find all documents containing any credit card numbers associated with a particular account holder or any emails containing specific data sent outside of the organisation from a particular email address.

Once a combination of search terms has been determined by the user, Critical Data Auditor can index all mails & documents found matching the search terms. More refined searches may then be rapidly executed against the indexed data.

## **System Requirements**

No software is required on the systems to be scanned. PixAlert Critical Data Auditor is designed to run from PCs. The minimum hardware and operating system requirements detailed below refer to the auditing computer and are NOT a requirement for target computers whose files systems are being audited.

### **PixAlert Auditor Hardware Requirements**

- Desktop PC;
- 2Gb RAM;
- 10 GB free disk space.

### **Operating System Requirements**

- MS Windows® XP Professional;
- MS Windows 2003 Server.

### **PixAlert Critical Data Auditor scans**

- Microsoft Windows® operating systems;
- Unix / Linux operating systems;
- Novell Netware;
- Microsoft Exchange, Lotus Notes, Novell GroupWise;
- Citrix Servers.

## **PixAlert**

Digital Hub,  
10-13 Thomas Street,  
Dublin 8,  
Ireland.  
+353 (0)1 7078860

## **PixAlert UK**

St. John's Innovation Centre,  
Cowley Road,  
Cambridge, CB4 0WS,  
United Kingdom  
+44 1223 421045

  
**PixAlert®**  
[WWW.PIXALERT.COM](http://WWW.PIXALERT.COM)