Top C-Level Challenges And Concerns
What keeps you up at night?

A survey by NASCIO asked C-level Executives that very question, and compiled a list of insomnia-inducing issues.

The top issues:
- Information Governance
- Information Security
- Data Lifecycle Management
- Compliance
- eDiscovery
- Archiving

Questions you should ask yourself are:
- Do I have an information management strategy in place?
- Do I have sufficient security to protect my company’s data assets?
- Am I effectively managing my organization’s data through sound information governance policies and best practices?
- Am I prepared to respond to litigation eDiscovery, expedited information requests, or regulatory audit?

These issues can be solved, but … Where do you begin?

These issues are not just limited to your department. They impact multiple departments across your organization.

This document will help you understand the challenges each organization has to secure, govern, retain and discover critical business information and how to solve these challenges.
IT Director
With your over burdened IT staff, rising costs, and ever-changing technology, you and your department are taxed more than ever before. Your major challenges and concerns are:
- Lack of IT Department Resources
- Increasing Hardware & Maintenance Cost
- PST Consolidation
- Data Lifecycle Management
- Ease of eDiscovery/Audit Export
- Management of Organizational Communication Data
- Employee Requests
- Employee Policy Provisions

Chief Legal Counsel
With the increasing information requests, litigation, and case assessments, the Chief Legal Counsel’s major business challenges are:
- Expedited Information Requests
- Complete Case Management
- Litigation Readiness Management
- Data completeness and ease of eDiscovery

Chief Risk/Compliance Officer
With recent SEC scrutiny, fines, and enforcement directed at the Chief Compliance Officer, it is now more critical than ever to ensure your organization is compliant and prepared. The CRCO’s major business challenges are:
- SEC Heightened Regulations
- Policy Enforcement
- Preparing for Audits
- Risk Mitigation
- Compliance

Chief Security Officer
With the increasing risks associated with email, social, IM, & mobile communication, you need a proactive solution to protect your organization. The CSO’s major business challenges are:
- Security Risk Mitigation
- Data Preservation
- Business Data Protection
- Ease of Data Access
- Protection from Reputation Damage

Human Resources
With the ever-increasing need to monitor, manage, and report policy violations in electronic communication, you need a solution to secure and retain every business conversation, contract and commitment. The major business challenges for HR include:
- Communication Oversight
- Employee Policy Enforcement
- Employee Case Assessment
- Protection from Employee Violations
- Prevent Internal Harassment
Your IT team is being pressured like never before to address requirements from departments across your business, despite your lack of resources and rising costs. For example, compliance requirements force you to evaluate PST consolidation and data lifecycle management concerns. Legal requires you to provide eDiscovery of electronic communication, and requests the ability to audit, export, and manage the data. Employee requests are increasing as your team spends hours trying to find lost and deleted email. Human Resources requires that you provide employee policy provisions, communication oversight, and that you help prevent potential employee misconduct on your network.

This means that your top priorities include reducing the strain on your IT department by consolidating PSTs and establish data lifecycle policies, educating employees on how to avoid risk, and empowering them with tools to rely less on IT. It also includes providing each department with the ability to quickly access, search, perform eDiscovery, and export your archived communication data without the need for IT, as well as establishing automated employee policy provisions and immediate violation alerts to mitigate risk.

Based on recent survey results, the following are your top IT concerns:

- **Lack of IT Department Resources** – Free up IT by enabling legal, auditors and other named users to independently conduct complete case assessment, eDiscovery, and data export without the need for IT assistance.

- **Increasing Hardware & Maintenance Costs** – Extend the life-cycle of your existing hardware investment by reducing data storage needs and the total number of servers needed to support your organization.

- **PST Consolidation** – Consolidate PST files to one searchable location and eliminate the need for PST file creation.

- **Data Lifecycle Management** – Create specific retention policies for all electronic communication, including email, social media, IM, and mobile communication data.

- **Ease of eDiscovery/Audit Export** – Easily export, redact, and encrypt communication data onto a flash drive, DVD, PDF, PST or stand alone archive viewer.
Management of Organizational Communication Data – Capture and comply with requests to utilize email, mobile, social media communication data.

Employee Requests – Allow employees to find their own archived data quickly and effortlessly by providing them a Google-like search for all email communication, social, IM, and mobile message data from one location.

Employee Policy Provisions – Educate employees on policies and how to avoid potential risks to themselves and the organization.

Business Case:

A major hospital in Boston, MA implemented a unified archiving solution, and was able to see an immediate ROI through reduced costs and a reduced burden on IT. The hospital empowered its employees by enabling them to access their communication data directly in the archive. By doing so, the hospital significantly reduced the amount of time and resources IT previously spent finding lost or deleted email. The hospital estimated that an average of 22 hours per week had been saved from searching for lost email alone.

Once implemented, the archiving solution provided the legal teams direct access to all of the hospital’s electronic communication data. This enabled them to quickly access the information, do a complete case assessment, eDiscovery, redaction, and data export without having to wait for assistance from IT, or continuing to go back to IT when data was missing. The hospital estimated an average savings of $26,000 per week in legal fees after having implemented this solution.

Archiving also brought the hospital into compliance with HIPAA and HITECH data security requirements. It ensured that protected health information (PHI) content was kept confidential, secure, and was not shared by doctors, nurses or other staff through social media or mobile communication. The archive allowed the hospital to have oversight on all electronic communication data, which helped eliminate inappropriate or harmful content, and reduced the risk of litigations costs by an estimated 23%.

Learn more about the solution this Boston hospital implemented, go to the final page of this document.
Chief Legal Counsel

Your organization must have the ability to respond to information requests, case assessments, and litigation at a moment’s notice. Your legal team needs to be able to quickly access, search, and perform eDiscovery on your archived communication data, and must provide organized, and accurate reports that can be exported in an easy-to-use format.

Based on recent survey results, the following are your top IT concerns:

**Expedited Information Requests** – Provide your legal team with access to all communication data when an expedited information request is received. They can access one central archive for all email, social media, IM, and mobile messaging data. There is no need for placing a request with IT. Direct access to the data means that your organization can meet expedited time restrictions, and can export and redact the data in a usable format.

**Complete Case Assessment** – Authorize management, individuals or legal teams to perform complete eDiscovery and case assessment audits without the need for IT involvement. These can be performed within an easy to use interface that shows all communication data across the organization in one location.

**Litigation Readiness** – Empower your legal team to prepare for litigation, or open records requests with direct access to the data. They can place litigation holds, perform eDiscovery searches, print, forward, save, restore, export and redact in one central location.

**Access & Search Data** – Allow named users to easily access all communication data from a web browser, and use the Google-like search function to access all electronic communication in one central location.

**Communication Data Export** – Export data with a flash drive, DVD, PDF, PST or use the standalone archive viewer.
Business Case:

Due to significant increases in expedited information requests, a major legal firm in Los Angeles worked with their clients to implement an organization-wide solution, within each client site, to preserve electronically stored information (ESI). The original driver for this project was to meet the recently updated guidelines of the United States Federal Rules of Civil Procedure (FRCP). This law requires that all electronic communication data including email, social media and mobile communications must be preserved "...in the anticipation or conduct of litigation." Failure to preserve and produce ESI during the discovery process can result in sanctions or dismissal of the action. Client communication data must be produced not only in an electronic or printed format, but it must also be provided in a mutually agreed upon readable format.

As the firm’s clients began to implement this solution, they saw immediate results. When clients received an information records request, they submitted it to the law firm. The law firm had specific administrator rights, accessed the client’s archive system, performed eDiscovery, compiled the report, redacted as necessary and exported it. This enabled the law firm to do complete case assessments, deliver complete reports on a specific issue or employee, and ensure their clients were ready for litigation. Each report included all employee communication in email, mobile, social media, search and IM data which helped to prove or disprove their case. These reports also eliminated the need for the legal firm to request information from the client’s IT department, or for them to have to work with anyone within the client’s organization.

This solution became a win-win for both the law firm and their clients. On average, the law firm was able to reduce response times for information requests by 60%, and enabled their clients to meet the expedited time restrictions set by the court. This also enabled the law firm to focus resources on more pressing issues, and to add new clients. As an added bonus, the firm’s clients who implemented the solution saw an immediate reduction in the burden on their IT department to respond to information requests. Each client also saw an average reduction in legal fees by 26%. In the end, the law firm found that they had increased client retention from 76% year over year, to 99%. So, by saving their clients money, they also increased their bottom line.

Learn more about the solution this L.A. Legal Firm implemented, go to the final page of this document.
Chief Risk/Compliance Officer

With the recent influx of additional SEC scrutiny, fines, and enforcement targeting the Chief Risk/Compliance Officer (CRCO), it is now more critical than ever before to ensure that your organization is compliant and prepared. At the heart of a compliance officer’s concern is the pursuit of enforcement actions under what is called the “Compliance Rule,” or Rule 206(4)-7 of the Investment Advisers Act. This rule requires that registered investment advisers adopt and implement written policies and procedures designed to prevent violations. This means you need to not only create and enforce policies, but you must also be prepared with a response if an enforcement audit arises, thereby mitigating your risk of violations and fines.

Based on recent survey results, the following are your top IT concerns:

- **SEC Heightened Regulations** – Create and enforce policies that will help you to be prepared if an enforcement audit arises.

- **Policy Enforcement** – Capture and monitor policy-violating communication including email, mobile messaging, and social media. Ensure employees are not sharing inappropriate or policy-violating content.

- **Prepared for Audits** – Empower administrators, auditors, and authorized users to perform essential functions, including regulatory searches and litigation holds, as well as to print, forward, save, redact, and export data.

- **Risk Mitigation** – Reduce the risks of potential violations before they occur within email, mobile data, social media, by monitoring and archiving communication in one central archive.

- **Compliance** – To meet compliance retention standards, organizations must securely archive email, social media, and mobile communication data all in one central location, plus prohibit message alteration or deletion, and be able to quickly access, search and export the archived data.
Business Case:

A major law enforcement authority in Baltimore, MD was recently subpoenaed by the Department of Justice in connection with a high profile case. The DOJ required this organization to produce all of their case-related information, including email, mobile, and social media data for specific employees involved in the case for the previous seven years. The difficulty was that the DOJ required this organization deliver all of the communication data to them in just seven days.

Fortunately, this agency already had a unified archiving solution in place that enabled them to easily retrieve the data, and provide it to the DOJ within the seven-day window. The communication data helped the Department Of Justice to both support and disprove specific aspects of the case. Without the proper solution in place, this type of request in the short amount of time would have been near impossible to accomplish. In the past this organization spent months trying to sort through employee’s locally “archived” PST files, from which they could only produce a fraction of the required data. Their results? Only email communication data. Now, at a moments notice, they are able to search, and export all their employee communication data quickly, easily, and in a simple-to-use format.

Learn more about the solution this Law Enforcement Authority implemented, go to the final page of this document.
Chief Security Officer

Your organization is being threatened like never before. Email, social media, and mobile communication data provide easy avenues for security risks and compliance violations. They also facilitate data leakage of sensitive or proprietary organizational information, and can allow employees to post inappropriate or malicious content. This is where a proactive solution can help you mitigate risk by educating your employees on what to avoid when using email, social media and mobile devices. A proactive solution can also help preserve and protect your business data, while providing users with easy access to their archived data. By implementing this type of solution, you and your organization are protected, and maintain compliance.

Based on recent survey results, the following are your top IT concerns:

**Security Risk Mitigation** – Mitigate security risks and avoid compliance violations by securely archiving email, social media, and mobile communication data all in one central location, allowing instant access to search and export of the archived data.

**Data Preservation** – Create specific lifecycle retention policies within your system to securely capture and preserve all electronic communication data. Manage the data based on policies with set time parameters to ensure the information is not altered or deleted.

**Business Data Protection** – Communication data must be preserved within an encrypted database and stored in a secure location. This can be either behind the corporate firewall, or in a certified cloud with redundant and secure data centers.

**Ease of Data Access** – Allow administrators, auditors, legal and other authorized users to access communication data from a web browser with the ability to perform regulatory searches, litigation holds, printing, forwarding, saving, redacting, and exporting functions with the built-in eDiscovery tools.

**Protection from Reputation Damage** – Restrict malicious or inappropriate message content, and prevent sensitive data from leaving your organization. Monitor, filter, block, and archive all email, social media, and mobile communication data.
Business Case:

A Financial Services corporation from New York, NY was concerned about maintaining compliance after several employee violations. They implemented a unified archiving solution that allowed them to set up policies that monitor social media accounts for certain keywords and terms. Once a violation occurred, an alert was sent to the network administrator.

After the organization implemented the solution, they were able to quickly identify the employees who were placing the organization at risk, and were able to block further violations. From there, it was very easy for the legal team to put together a complete case assessment of all the individuals involved in the violations. By blocking the damaging content, it prevented inappropriate messages from being posted or shared online, ensuring that sensitive data did not leave their organization. Since the solution was implemented, no policy violations have occurred, and of the attempted violations, zero have been successful. This solution has kept the organization’s information safe, secure, and completely compliant with all FINRA and FRCP rules.

Learn more about the solution this Financial Services Organization implemented, go to the final page of this document.
Human Resources includes many moving parts, involving complex issues that you need to address in any given day. Managing employee benefits, retirement plans, grievances, compliance issues, and harassment claims are just the beginning. The latest hidden threat to HR is employee use of email, and social media to transmit any message, at any time. This has created an environment where it seems impossible to track who says what, to whom, and when.

It has become essential to securely monitor and retain every business conversation, contract and commitment. In addition, you should have complete communication oversight into what your employees are discussing to ensure policy enforcement. You should be aware of what your employees are texting, what they are posting on social media, and what they are saying via email. This is where implementing a software solution that provides complete communication oversight, policy enforcement, employee case assessment, message retention, and protection from reputation damage can resolve these issues.

Based on recent survey results, the following are your top IT concerns:

**Communication Oversight** – Execute a search of all archived communication data for keywords to gauge the tone and theme of employee communication. Set up alerts for keywords and phrases that violate policy. Monitor and archive social media content.

**Employee Policy Enforcement** – Ensure employees are not sharing inappropriate content, or transmitting policy-violating information. Establish communication policies and enforce them with keyword alerts, monitoring, filtering and blocking.

**Employee Case Assessment** – Allow authorized individuals or legal team members to perform complete eDiscovery and case assessment audits without the need for IT involvement.

**Protection from Employee Violations** – Prevent users from posting inappropriate or policy-violating information in social media by monitoring and archiving communication data.

**Prevent Internal Harassment** – Prevent harassment, bullying, and other inappropriate content by having oversight of electronic communication by using keyword alerts and filters.
Business Case:

An major educational organization from Austin, TX discovered that employees were targeting certain individuals within their organization, and engaging in inappropriate, bullying, and malicious communication. Unfortunately, management was having a difficult time catching the employees in the act. Many times the content was posted in social media, and was quickly deleted shortly thereafter. With no physical record of the damaging content, the company had no proof of the violations. They needed to find a solution that could capture all of their employee electronic communication data, so that they could search the results and have conclusive evidence.

Once the company researched, purchased and implemented the solution, they set up policies to begin monitoring employee communication data, based upon the keywords used in previous attacks. When the inappropriate communication occurred, a pop-up message appeared on the employee's screen stating, “This post is in violation of organizational policy.” The text and metadata of the social media post was captured, and archived, and an alert was sent to the network administrator. From there it was very easy for the HR team to piece together what was said, to whom, and which individuals were involved. HR was able to quickly resolve the problem and prevent any future misdeeds within their organization.

Since the implementation of this solution, the organization has been able to monitor, and archive all email, social media, and mobile communication data. The unexpected benefit of this software implementation, was that the organization could filter and block employee access to inappropriate websites, and had a record of all attempted searches. This provided a means for the organization to find violators of their employee contract and communication policy, notify the individuals of the violation, and eventually prove cause to terminate them.

Since implementation of the software solution, the organization has successfully prevented all inappropriate content from leaving the company’s network. This has mitigated their risk for harassment claims, and has provided powerful evidence to defend the organization from wrongful termination lawsuits. They estimate an overall decrease in litigation and claims costs by more than 83%.

To learn more about the solution this educational organization implemented, turn to the next page.
About Retain

Retain provides unified archiving of all business communication including email, social media, and mobile communication data for case assessment, search, and eDiscovery. It can be deployed on-prem or in the cloud.

Retain is a unified archiving suite primarily focuses on email archiving for Microsoft Exchange and Office 365, but it also includes comprehensive native support for archiving Gmail and GroupWise email. In addition to email archiving, Retain supports the archiving of electronic business communication including data created on mobile devices, social media. Retain Mobile archives mobile device communication data for Android, BlackBerry, and iOS, including SMS/text messages, BBM Messages, BBM Protected, phone call logs, and PIN Messages. Retain Social provides monitoring and data insight into message context and tone of all posts for Facebook, Twitter, YouTube, LinkedIn, Instagram, Vimeo, Flickr, Pinterest, and Google+ (on and off network).

Best Overall Value and Champion

Retain was recently awarded as the Best Overall Value and Champion of Content and Email Archiving in the Info-Tech Vendor Landscape report. The report stated that, “...on a relative basis, GWAVA maintained the highest Info-Tech Value ScoreTM of the vendor group. Vendors were indexed against GWAVA’s performance to provide a complete, relative view of their product offerings.” “GWAVA has the best value for highly regulated enterprises through the best practices information for financial and healthcare.” Info-Tech went on to call Retain, “The most complete product at its price point.”

About Micro Focus

Micro Focus is a global software company with 40 years of experience in delivering and supporting enterprise software solutions that help customers innovate faster with lower risk.

By applying proven expertise in software and security, we enable customers to utilize new technology solutions while maximizing the value of their investments in critical IT infrastructure and business applications. As a result, they can build, operate, and secure the IT systems that bring together existing business logic and applications with emerging technologies—in essence, bridging the old and the new—to meet their increasingly complex business demands.