

The Business & Technology Challenges of Electronically Stored Information (ESI)

Why the Content Archiving Architecture matters...

NAYATEK

One Liberty Place
1650 Market Street, Suite 3600
Philadelphia, PA 19103, USA
Tel: +1-302-452-8422
Fax: +1-610-429-4216

NAYATEK EMEA

Cº Cerro de los Gamos, 1 Edificio 1
28224 Pozuelo (Madrid), Spain
T. +34 91 790 12 00
F. +34 91 790 12 90

Table of Contents

Executive Summary.....	3
The ESI Challenges	4
Volume of ESI and the IT Challenge	4
Legal Implications of ESI.....	6
ESI and Compliance.....	8
The Solution	10
Barriers.....	10
Policies	11
Technology.....	12
The Architecture Matters.....	12
The Solution Checklist.....	13
Solution Platform Architecture	14
Content Archiving	14
EDiscovery.....	14
Storage Management	15
Business Continuity.....	15
Compliance	15
Total Cost of Ownership	16
Summary	16

Executive Summary

No organization is immune to the explosive growth in the volume of electronically stored information (ESI). The rapid growth of ESI is having a tangible impact upon organizations in three primary areas, the volume of ESI upon the IT infrastructure, the legal implications and regulatory compliance. The impact of ESI upon corporate networks, infrastructures and email servers is burdening already strapped IT staff, impacting user productivity and driving up costs. Laws, regulations and company policies establishing the legal status, mandatory retention periods and discoverability of ESI have real consequences for organizations and virtually assure its rapid growth rates for the foreseeable future.

ESI exposes organizations of all sizes to legal risk. EDiscovery is now a reality for all organizations as there is no such thing as a lawsuit or internal investigation that doesn't involve at least some EDiscovery. Furthermore, no part of the global economy is immune to the impact of regulatory or legal compliance which often require organizations to capture, store and be able to respond within relatively short timeframes to legal discovery requests. So knowing what ESI you have, where it's located, who can access to it and how to search against it quickly & efficiently can significantly reduce the time, cost and effort required to respond to a legal discovery requests or internal investigations is essential.

What is clear is the challenges of ESI are not going away nor is there a silver bullet solution. As a result, the development of an overall ESI strategy is a baseline requirement today. Organizations that do not have an ESI strategy are placing themselves at a serious disadvantage. As the volume of ESI increases exponentially each year, the failure to get started on an ESI strategy only makes matters worse. Lost time due to non-existent, inefficient or poorly executed ESI strategies means lost money, sanctions and lost legal cases.

The bottom line is management needs to take ownership of the strategy to ensure it is implemented and enforced. An effective ESI strategy combines the development of written policies and procedures combined with the appropriate technology to implement and enforce them can evolve over time to reflect the business, legal, compliance and technological landscape where an organization resides. Forward looking organizations focus on those areas they can address today but leave the door open to add in those additional components they know may be of importance in the future.

Today the stakes are much too high to make the wrong technology choice. Selecting a technology solution provides a platform to build on, can help future proof against changes in legal requirements, new ESI data formats, retention requirements and the ever encroaching impact of regulatory compliance is critical. An integrated content archiving solution with comprehensive EDiscovery, storage management, business continuity and compliance functionality can serve as the foundation of an ESI strategy to effectively capture, index, store, secure, manage, retain and discover disparate ESI. While the whole range of functionality may not be necessary today, an integrated solution built for the ESI challenges of today and open to those of tomorrow allows an organization to maximize the value of the investment and lower the total cost of ownership. Getting control over your ESI no longer has to be so complicated.

[3]

The ESI Challenges

The challenges of ESI impact an organization in three primary areas, the volume of ESI upon the IT infrastructure, the legal implications and regulatory compliance. Each of these challenges will have varying impacts upon an organization depending upon factors such as size, location and industry. These challenges rarely manifest themselves equally within an organization. However, whether on their own or combined in some manner the challenges of dealing with ESI are real, often complex and will not go away on their own. Delays in addressing the challenges will only serve to compound the problem and the overall cost of a solution.

Volume of ESI and the IT Challenge

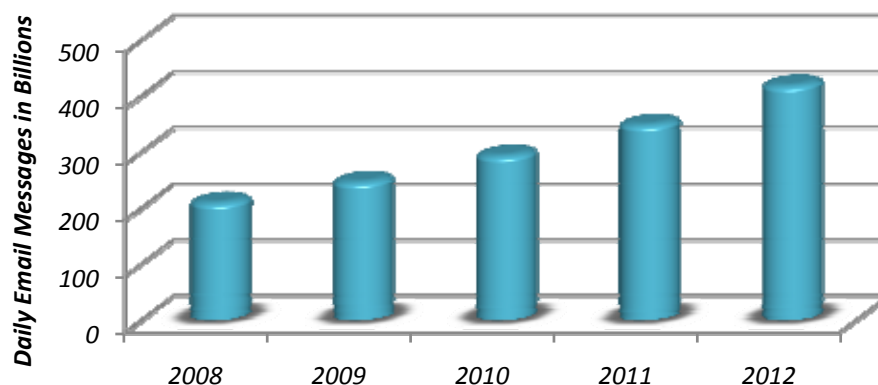
ESI is increasingly placing serious burdens on email servers, files servers, portals and other application servers impacting performance, management and driving up costs. Laws, regulations and company policies establishing the legal status of ESI, mandatory retention periods and its discoverability have exponentially impacted the volume of ESI and virtually assured it rapid growth rates for the foreseeable future. The reliance on ESI has grown irreversibly and as a result, no organization is immune to the challenges it has created.

"By 2011, the digital universe will be 10 times the size it was in 2006"

The Diverse and Exploding Digital Universe, An Updated Forecast of Worldwide Information Growth Through 2011, March 2008, An IDC White Paper sponsored by EMC

Organization's often take the easiest course of action to try and address the challenge. They simply buy more storage, try to optimize it and/or impose policies that attempt to limit the amount of ESI in the organization. While more storage capacity always helps, it's an inefficient and band-aid approach by itself. Policies often force premature deletion of ESI and create more end user housekeeping, impact user productivity and increase risk by forcing corporate content out of the organization's control.

Worldwide Email Traffic



SOURCE: The Radicati Group, a technology market research firm.

While increasing storage capacity is a fact of life for all organizations, managing ESI across different silos can be complicated, costly and less than optimal. Decentralized control of ESI complicates the implementation of policies, security, search & index, and access control. The process of storage optimization can alleviate some of the pain by moving ESI from primary storage to less expensive secondary storage. This takes the immediate burden off email servers, file servers, portals and other application servers allowing them to run at peak efficiency reduce downtime and the chance of failure.

However, storage optimization is about more than just moving ESI from one location to another. Managing the volume of ESI requires the ability to automatically and consistently capture, archive, secure, store and retain the ESI you have created at the source in a seamless and effective manner. A comprehensive solution is often a necessity for organizations to get back in control of their ESI. The development and implementation of an ESI strategy is the foundation of a comprehensive solution.

The volume of ESI has clearly impacted organizations and IT departments

- Performance degradation of email servers, file servers, portals etc...
- Poorly optimized and silo based storage of ESI
- Poorly indexed and difficult to search ESI
- No ability to automatically capture and archive ESI
- ESI is duplicated , uncompressed and unsecure
- ESI access control is limited with no audit control
- No centralized ability to set and enforce retention policies

Organizations that do not have an ESI strategy and the appropriate technology in place to ensure its implementation are placing themselves at a serious disadvantage. An ESI strategy does not require the complexity of a records management (RM) or enterprise content management system (ECM). Rather it is more appropriate and effective to use an integrated content archiving platform as the technological foundation. It is substantially less complex and typically operational in a fraction of the time. It can ensure ESI is captured before it has been modified or deleted and ensure its authenticity. Once ESI is captured, it is fully indexed and becomes searchable for the organization.

An integrated content archiving platform through compression and single instance storage can realize substantial savings in the amount of total storage. With support for industry standard storage protocols, scenarios (federated, storage clusters, redundant, cloud etc...) and devices, organizations can maximize resources. Furthermore, its ability to set and enforce retention policies brings a much needed level of structure to managing the ESI lifecycle. Knowing the size of your ESI, where it is stored securely and when it will be deleted is fundamental to storage management. An ESI strategy with the right technology foundation can decrease the IT workload, use fewer resources and serve as a major step forward for an organization to get back in control of its ESI.

Legal Implications of ESI

EDiscovery is now a reality for all organizations. There is no such thing anymore as a lawsuit or internal investigation that doesn't involve at least some EDiscovery. ESI contains contractual, financial, operational and human resource information and can expose all organizations, regardless of size to legal or regulatory compliance risk. In today's regulatory and legal environment, no organization is safe from litigation. The evidentiary weight of email and other ESI is now clearly recognized in most countries.

Organizations are increasingly aware of the growing burden of ESI. Many also understand ESI is no longer considered to be just email and as such, other content sources such as files, instant messages, text messages, voicemail, portals, and other emerging applications will need to be discoverable. Organizations need to be prepared to run rapid internal investigations, develop pro-active litigation readiness strategies and to respond quickly to EDiscovery requests sometimes in as quickly as 24-48 hours.

Knowing what ESI you have, where it's located, who can access to it and how to search against it quickly & efficiently can significantly reduce the time, cost and effort required to respond to a legal discovery requests or internal investigations.

The Federal Rules of Civil Procedure updated in December 2006 in the U.S, eliminated the traditional excuses companies have used for not being able to find ESI. Legal discovery requests must now be answered rapidly and thoroughly and excuses can result in fines and sanctions. The sheer volume of ESI and tight timelines to respond to legal requests means organizations can no longer rely on basic search and retrieval technology, backup tapes and manual processes. Organizations need to ensure they capture their ESI, retain it, secure it and retrieve it within a short period of time

- In the past three years, 81% of IT departments have been required to search back-ups to retrieve one or more emails (Osterman)
- 4 out of 5 users employ personal/local archives to store messaging system data (Osterman)
- Almost 50% of organizations have been ordered by a court or regulatory body to produce email (Osterman)
- The most common single reason for disciplinary action is the sending of unauthorized emails (CIPD UK)
- 42% of staff don't know that email harassment of colleagues could land their employer in court (DataSec)

Some organizations make it their company policy to delete any ESI older than 90 days from their email servers or they allow their users to determine what should be archived and what should not. As long as they comply with their policy, there is nothing to worry about, right?

However, the content in those emails continues to live even after it has been deleted. Although the internal copies of emails may have been deleted, copies of it or the original could be in the hands of an external business partner, client or individual. If the email contained contractual promises, price offers, or other statements obligating the company to perform services or provide products, it's very doubtful a court will absolve a company of its obligations just because they followed their policy. Having a copy of those

messages and the message thread can ensure that emails are not taken out of context and used against the company. Proper preparation and defense in the event of legal situation or compliance audit is always preferable to the unpleasant surprises of being woefully unprepared.

Organizations that do not have an ESI strategy are placing themselves at risk. A strategy that governs the archiving, storage, retention and discoverability will reduce legal risk. In the event of a legal discovery request or an internal investigation, the organization's legal counsel must have the ability to make an informed decision about how to proceed.

Organizations that have trouble responding effectively and on a timely basis to EDiscovery requests have many of the following characteristics:

- Lack of a centralized archive or data repository
- ESI is located only backup tapes which are very difficult to search
- Poorly indexed ESI
- Poor or old search and retrieve technology
- Lack of IT and Legal resources
- Inability to demonstrate a defensible chain of custody

Without an understanding of the relevant ESI, where it is located, who has had access to it and how to cull it down, it is extremely difficult to make an informed decision regarding the merits of a case. What actually are the risks? What don't they know that could be hiding in their ESI? Will their inability to respond quickly to EDiscovery requests be seen as trying to hide information? Should they settle the lawsuit or investigation out of court? Should they defend themselves and go to trial?

An effective ESI strategy is about more than storage and enterprise search. It requires the ability to provide specific privileged users with audited access to perform federated searches across the archives, create investigation folders, cull down results and eventually be able to export these folders. Given that ESI can be tangible evidence in a legal inquiry, it is critical that it is handled with care. A system that ensures the original content cannot be deleted or modified can demonstrate an organization has correctly handled its ESI and thus reduce its risk. Granular role definition for access to the archives, a forensic security model with comprehensive auditing and full encryption of the archives are essential.

The bottom line is management needs to take ownership of the strategy to ensure it is implemented and enforced. The cost of responding to an EDiscovery request is more than the time spent to search for results, it's the ability to make informed decisions that can reduce risk and preserve the organizations assets. Organizations that choose to get back in control of their ESI will emerge stronger, better placed to protect their ESI assets and will realize costs savings and increased efficiency.

ESI and Compliance

The impact of regulatory compliance upon ESI is a business reality. Regional, national and local governments have increased their efforts in recent years to ensure corporate transparency and accountability. The current economic climate all but ensures a coming wave of new regulatory compliance provisions which will cast an even wider regulatory net affecting significantly more organizations. However, regulatory compliance can be a confusing alphabet soup of complex regulations, vague interpretations and vendor driven fear, uncertainty and doubt. Its applicability often depends upon the specific industry, jurisdiction and the geographical footprint of the organization. So it's perfectly understandable that organizations often face great difficulty to determine specifically where, what and how to comply with regulations such as Sarbanes-Oxley (SOX), SEC Rule 17a-4, UK FOIA, European Data Protection Acts, GLBA, HIPAA, FDA 21 CFR Part 11, German HGB and GoBs.

If a company is in a highly regulated industry, is a public company or must adhere to specific local or regional regulations, typically there are mandates stipulating a minimum retention periods (ex: 3,5,7 or 10 years) for ESI, not a maximum period. These are just minimum retention periods and often an organization's policies supersede regulations in order to best protect their interests and minimize overall risk. Retention periods often need to be set for the specific departments, content types and users within the organization.

Many organizations are placing themselves at risk and are not prepared to deal with the internal policy or regulatory compliance impact of ESI.

- Lack of a centralized archive or data repository
- Cannot guarantee capture of ESI
- ESI is stored in clear text
- Very difficult to respond to audit requests & investigations
- No audit trail on ESI access, modification or deletion
- Inability to demonstrate internal policy or regulatory compliance
- No way to enforce retention policies

Organizations in highly regulated industries or who have multinational operations are already accustomed to the regulatory compliance burden of ESI. However, the majority of organizations often do not have direct regulatory obligations and as a result they often choose to do nothing. What these organizations do have, are internal policies and governance dealing with everything from HR policy to email usage. Having a policy that deals with ESI yet provides no enforcement or assurance the policy is being followed can be even worse than not having a policy at all. The organization is still responsible and failure to meet regulations, legal requests and often adherence to its own policies can have serious consequences ranging from substantial fines, to unwanted exposure to criminal prosecution and possible punishment as well as drops in their share price if they are a public company.

The lack of a retention policy or even premature deletion policies does not eliminate responsibility. All ESI is not created equally and organizations need to determine the priority and the risk of their ESI. During the retention period, they must ensure that the ESI is available, readily searchable and can be quickly produced at any point. In the absence of any clear directions on data retention the retention policies can also be used as a way of simply controlling the size and rate of growth of the archive.

However, simply storing and retaining ESI alone does not establish its validity and authenticity. Whether dictated by industry regulations, government requirements, by company policy, or a combination of factors all organizations must adhere to some level of compliance. The development of an ESI strategy details the processes and how they will be enforced by the technology and systems the organization has put into place.

Data Retention example:

**Compliance
& Retention
Requirements**

- **ACME Company**
 - Ensure that all email messages are captured and archived
 - Different retention periods for different users
 - Management: 7 years Finance: 7 years Organization: 3 years
 - Encrypted Archives with fully Forensic Audit Trail
 - Prevent User Deletion
 - Auditor Approved Deletion

The compliance impact of ESI affects both organizations in heavily regulated industries as well as those without regulation. Organizations that are impacted by regulatory compliance must determine how those regulations affect them and in many cases the best strategy is to set your internal standards higher than what is expected from you by regulation. All organizations however have internal policies and the risk of not enforcing and adhering to those policies can have repercussions.

Organizations often hesitate to move forward as compliance is seen as a sunk cost with no real ROI. However, when compliance is part of an effective archiving and information retention strategy those costs are rolled up into the larger project where ROI is clear and constant. The ability to guarantee capture of ESI, ensure it is stored in its original format, cannot be modified or deleted, ensure it is encrypted to provide security, can be retained for a pre-determined amount of time and demonstrate compliance through a fully forensic audit trail are key pillars of an ESI strategy.

The Solution

An overall ESI strategy combines the development of written policies and governance plans with the appropriate technology needed to implement and enforce them. Organizations realize the challenges of ESI are not going away nor is there a silver bullet solution. ESI impacts virtually every business area. As a result, often a cross departmental and cooperative approach is recommended as it shares accountability and responsibility across the organization. In this way there can be agreement on the written ESI policies and the appropriate technologies.

However, in many organizations this may not be possible as the challenges of ESI often do not manifest themselves equally. The volume of ESI may be the biggest challenge in one organization while compliance issue is of paramount importance in another. An ESI strategy is a living strategy composed of policies, procedures and technologies that evolves over time to reflect the business, legal, compliance and technological landscape where an organization resides. Forward looking organizations focus on those areas they can address today but leave the door open to add in those additional components they know may be of importance in the future.

Barriers

Surprisingly, many organizations do not have an ESI strategy in place. While they may recognize the need to implement a strategy, the barriers to doing so often get the best of them. The barriers are often times substantial, costly and difficult to overcome. As the volume of ESI increases exponentially each year, the failure to get started on an ESI strategy will only make matters worse. Lost time due to non-existent, inefficient or poorly executed ESI strategies means lost money. The impact can grow beyond impacting user productivity to include fines, sanctions and lost legal cases.

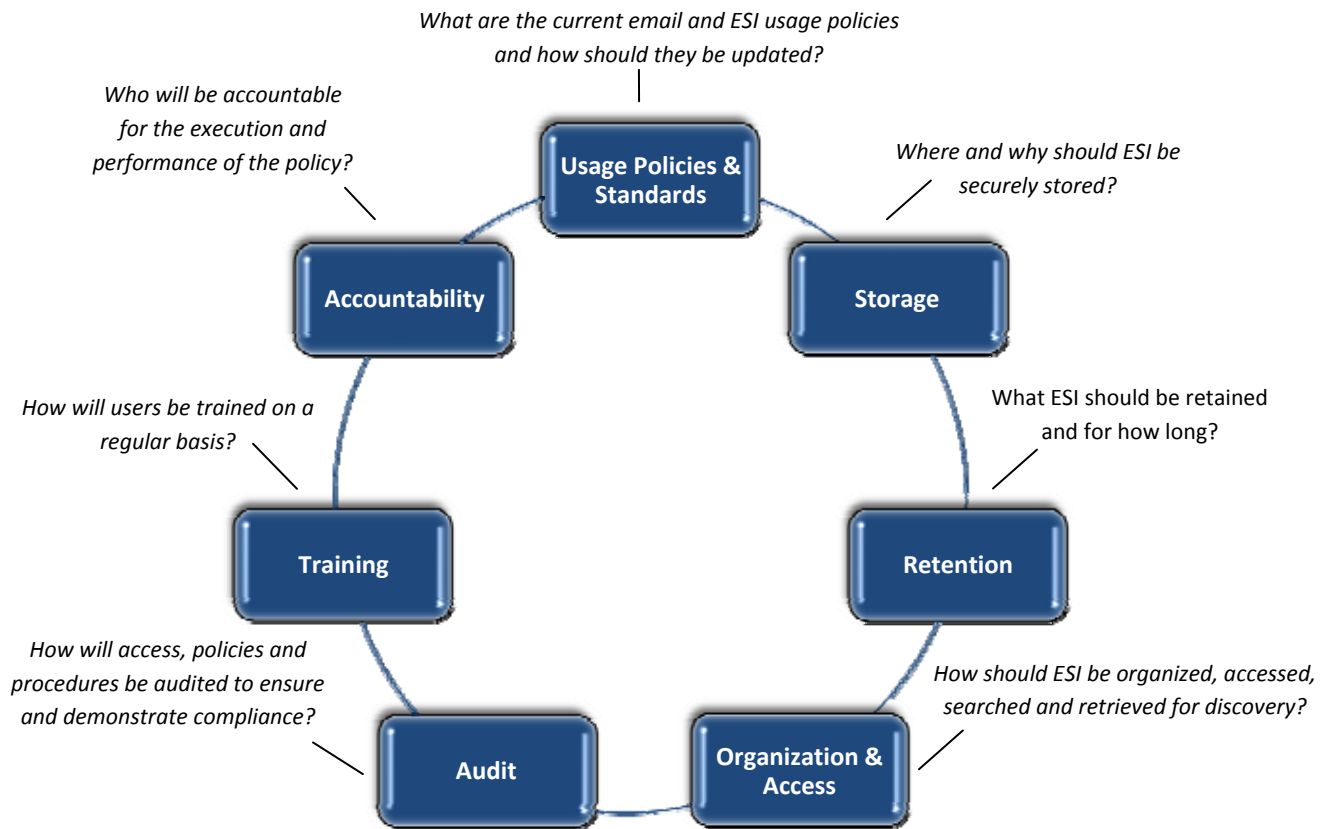
Common Barriers to implementing an ESI Strategy

- Lack of time and resources
- Budget is unavailable
- Ownership and accountability of the project
- No one has an understanding of what needs to be done
- No one wants to take responsibility
- Legal advice is either insufficient or confusing
- Volume of ESI is unmanageable
- Technology choices are complex and confusing

However, the focus does not need to be on simultaneously overcoming these barriers. With the right high level policy focus and the selection of the appropriate technology that can grow with the organization, the ability to implement a solution today and enhance it over time is often the recommended solution.

Policies

While each organization will have its unique requirements, typically an ESI policy would include at a minimum many of the following components. Subsequently specific policies, procedures and technology solutions would be defined within each area in order to ensure implantation and enforcement.



The objectives of ESI policies may differ from organization to organization but are likely to include many of the following:

- Clearly defined and structured ESI archiving and retention process
- Reduce the burden on the IT infrastructure, email servers & application servers
- Increase system performance and optimize storage
- Increase user productivity and help to improve the bottom line
- Minimize legal and regulatory risk from ESI
- Increase ability to respond rapidly to legal and EDiscovery requests
- Demonstrate compliance against company policies and external governance

Technology

An integrated content archiving solution can serve as the foundation of your strategy to address the challenges of ESI. Any strategy should strongly consider solutions that can provide strong functionality in terms of content archiving, EDiscovery, storage management, business continuity and compliance. While the whole range of functionality may not be necessary today nor apply to the current ESI strategy, an integrated solution will save you considerable time, effort and money especially as your ESI strategy evolves. An integrated solution built for the ESI challenges of today and tomorrow allows your organization to maximize the value of its investment and lower the total cost of ownership.

Organizations are faced with a wide range of possible technology choices. Many are point solutions developed for specific ESI formats, others only provide EDiscovery functionality and still others promise to deliver a full content archiving solution. The endless list of available solutions with their often similar feature sets, claims and promises only serves to add to the confusion and complexity of selecting a solution that makes sense for an organization.

The Architecture Matters

When considering an integrated content archiving solution one needs to think about the future. Needs and requirements will evolve, new data formats will be created, new regulations will be mandated and options like redundancy, business continuity and disaster recovery may become necessities. In selecting a solution, the importance of the product architecture should never be underestimated. While features from vendor to vendor often blur together, it is the underlying architecture of the solution that is most critical. The architecture leverages or limits the feature set.

The architecture ensures core functionality is available in all scenarios without compromise or caveats. It does not limit configuration or deployment options nor outsource core functionality and create dependencies on third party systems. In critical areas such as single instance storage, search & indexing, integrated redundancies and security & compliance, the difference becomes very clear. The architecture is the foundation upon which all of the functionality is built and should be as flexible, adaptable, and scalable as possible.

However when customers in the face of clear ESI challenges are slow to adopt existing solutions and prefer to delay projects and suffer the consequences one has to wonder about these solutions”?

- Are they meeting customer needs and requirements?
- Are they based on old architecture and technology?
- Are they poorly retrofitted for today’s realities?
- Are they easy to evaluate and implement?
- Are they cost prohibitive? ...too many hidden costs?
- Do they require too many resources to run and maintain?

What is clear is it's a big challenge for products whose architectures were developed in the late 1990's to keep pace with growing challenges of ESI. Things were much simpler back then. Today's ESI volume, the reality of EDiscovery and the burden of compliance have demonstrated the inadequacies of these older product architectures. While vendors of these solutions have "bolted-on" new functionality, it has served to further increase the IT management burden. Furthermore the scalability, availability and performance of these systems under the weight of new conditions have often become problematic.

<p style="text-align: center;">Antiquated & Limiting Architectures</p> <ul style="list-style-type: none"> ▪ First generation vendors still use their 1990's designed architectures ▪ Designed in a "pre-compliance" and "pre-legal discovery" era ▪ Evolved by "bolting on" and "retrofitting" new features ▪ Many more recent products use the same architectural blueprint 	<p style="text-align: center;">Significant Dependencies & Points of Failure</p> <ul style="list-style-type: none"> ▪ Outsource core functionality to MS SQL servers & IIS servers ▪ No integrated redundancy & high availability ▪ More friction points equals more points of failure ▪ Special product architectural needs forces changes to the client environment 	<p style="text-align: center;">Complex, Costly & Cumbersome to Install & Manage</p> <ul style="list-style-type: none"> ▪ Long lists of pre-requisites ▪ Complicated installation requires vendor ▪ New skill sets and significant training often required ▪ More moving parts and dependencies ▪ Considerable ongoing maintenance and management 	<p style="text-align: center;">All Feature Sets are Not Created Equal</p> <ul style="list-style-type: none"> ▪ Many vendors have similar feature sets on paper ▪ The Architecture has a direct impact on the ability to fully leverage the feature set ▪ Limited by the product's scalability, and performance ▪ New functionality is "bolted on" instead of "built-in" ▪ Security & compliance functionality is an after thought
---	---	--	---

Today the stakes are much too high to make the wrong technology choice. Requirements have changed and old product architectures leave a lot to be desired in terms of scalability, performance and ongoing maintenance

The Solution Checklist

The following "Solution Checklist" provides a targeted list of solution features, functionality and components to look for when evaluating and integrated content archiving solution to serve as the foundation of your strategy to address the challenges of ESI. Any strategy should strongly consider solutions that can provide strong functionality in terms of content archiving, EDiscovery, storage management, business continuity and compliance. While the whole range of functionality may not be necessary today, an integrated solution will save you considerable time, effort and money down the road. It allows an organization to maximize the value of its investment and lower the total cost of ownership.

Solution Platform Architecture

The core platform architecture is what matters most. If the foundation is old, limited, outsources core functionality to external applications or is not fully optimized for its feature set, one needs to be very careful. The product's architecture plays a critical role in how the features and functionality are leveraged. Don't lock your ESI into old product architectures, prioritize the following capabilities:

- ✓ Grid or dynamic next generation architecture allowing the virtual overlay of the existing network infrastructure, rather than trying to imposing changes in the environment
- ✓ Capability to distribute processing resources globally
- ✓ Easily scale performance by adding additional servers & storage without taking down the system
- ✓ Highly optimized to leverage the entirety of the feature set
- ✓ Scalability and data availability do not have to depend upon external databases
- ✓ Distributed operation with secure encrypted digitally signed network communications
- ✓ Open, standards based, modularly designed and built with an eye on the future

Content Archiving

A robust content archiving platform built on a data neutral engine with powerful and optimized search and index technology provides a platform that can benefit organizations of all sizes. While email is typically the first type of ESI to be addressed, the ability to add capabilities to archive content on files servers, portals, instant messages and other data formats should not be overlooked. Look for the following functionality:

- ✓ Robust capability to ensure the capture, security, integrity and privacy of ESI
- ✓ Data Neutral Design
- ✓ Optimized modern Indexing and search technology
- ✓ Ability to full text index hundreds of file types...if you can't index it, you can't search for it
- ✓ Improve End User Productivity through self service robust search and recovery functionality
- ✓ Powerful stubbing provides users with an infinite mailbox and no need for inbox housekeeping
- ✓ Improved application server (MS-Exchange, File Servers etc...) performance

EDiscovery

EDiscovery for external or internal requests and investigations is a reality for all organizations. An effective solution allows organizations to get their electronic house in order to proactively prepare for these requests. The following functionality should be a minimum requirement:

- ✓ EDRM based solution
- ✓ Modern, highly optimized federated search & index fully leveraged the product architecture
- ✓ Full text indexed content including attachments and files without compromises
- ✓ Complex multilevel search capabilities
- ✓ Investigation and case management functionality to manage, tag, cull down and export results
- ✓ Granular legal hold can be applied to individual messages and investigation folders

Storage Management

Rapidly increasing volumes of ESI have brought storage management and storage optimization to the forefront. An effective solution has an open storage layer where standard storage devices or solutions can be integrated and used in more than just simple configuration scenarios. Flexible storage options such as the following provide organizations with the capabilities that “fit” their organization:

- ✓ Flexible archiving policy & powerful stubbing of ESI offloads storage to lower cost secondary storage
- ✓ Open Storage Layer works with what the organization already has by supporting a wide range of storage options (Local, DAS, SAN, NAS, CAS, iSCSI and other devices via NFS/CIFS)
- ✓ True Global Single Instance Storage
- ✓ Compression rate of at least 40-50% of actual office user data sets including the full-text indexes
- ✓ Federated Storage capabilities & Cloud storage options
- ✓ Eliminate or reduce the usage of PST files
- ✓ Provide location independence by abstracting the physical location of the data

Business Continuity

Business continuity is no longer a concern for only the largest organizations. Prioritize functionality that can ensure the availability, security, integrity and management of your ESI:

- ✓ Integrated Redundancy no longer needs to be a nice to have option
- ✓ Solutions that provide integrated redundant & disaster recovery configurations
- ✓ Disaster Recovery scenarios can be implemented without the need for complicated external tools
- ✓ Redundant storage of archived ESI can prevent data loss and provide much faster recovery scenario
- ✓ Easy to use entire archive, mailbox and message restore functionality is a baseline
- ✓ Fewer points of failure (i.e....external dependencies)

Compliance

Compliance and security functionality “built-in” to the system rather than bolted on at a later date is inherently stronger. The following integrated functionality ensures the security of ESI and provides the ability for an organization to demonstrate compliance:

- ✓ Solutions with organizationally driven methodologies provide the best alignment of an organization’s business, risk and IT objectives
- ✓ “Built-in” Forensic security model with comprehensive audit trail
- ✓ Secure access control of the archives through highly granular user roles dictate actions and access
- ✓ Ability to demonstrate compliance through a historical record of what has been done with the archives
- ✓ Flexible and audited Data Retention policies to enforce message retention policies
- ✓ A secure, encrypted, tamper resistant archive can ensure discovery is legally valid and admissible

Total Cost of Ownership

Vendor supplied ROI formulas or cost savings projections make calculating total cost of ownership (TCO) complicated at best. These calculations even if they are validated by third parties, apply to specific conditions and circumstances and are always up for discussion. When comparing solutions it becomes even more difficult as features and functionality often blur together. The TCO calculations that really count are those that can logically be based on common sense assumptions. Does it pass the common sense smell test? Solutions that do what they are supposed to do and require less time, money, resources and effort that need to be expended, have lower levels of TCO. Look for the following:

- ✓ Ease of evaluation and installation with a downloadable enterprise solution is key
- ✓ Solutions that require vendor installation or evaluation assistance are likely to be resource intensive
- ✓ Fewer external dependencies, and prerequisites are easier to use, manage and maintain
- ✓ Software delivery and installation models makes it easy to evaluate, deploy and manage the solution
- ✓ Integrated redundancies can eliminate the need for 3rd party clustering tools
- ✓ Solutions that reduce the overall overhead and reduces the points of failure
- ✓ Look for green solutions that use less hardware or those that can take advantage of virtualization

Summary

As you look to address the challenges of ESI and look to the horizon, one thing is very clear, ESI is not going away and avoiding the challenges will only complicate things down the road. In fact, delays in addressing your ESI challenges will most likely be far more costly than tackling the problems today. There are solutions on the market that can help you future proof against changes in legal requirements, new ESI data formats, retention requirements and the ever encroaching impact of regulatory compliance. The complexity introduced into the market by many vendors has in many cases held organizations back. Getting control over your ESI no longer has to be so complicated.

Pay special attention to those solutions meeting the following requirements...

- ✓ *Integrated solution with Content Archiving, EDiscovery, Storage Management, Business Continuity and Compliance functionality*
- ✓ *A solution that can easily grow with your evolving requirements.*
- ✓ *Natively encrypted archives & a forensic security model with a comprehensive audit trail*
- ✓ *An open storage layer that doesn't force changes on your organization*
- ✓ *Integrated redundancies that provide for business continuity and disaster recovery*
- ✓ *Ease of installation, configuration and management*
- ✓ *TCO that passes the common sense smell test*
- ✓ *And a highly optimized grid or next generation optimized architecture to make it all possible*