INFORMATION OVERLOAD:
HOW TO SECURE AND MANAGE IT TO YOUR COMPETITIVE ADVANTAGE
A SYMANTEC SURVEY OF IT MANAGERS CONDUCTED BY APPLIED RESEARCH IN SEPTEMBER 2008 FOUND THE FOLLOWING:

- 85 percent rated protecting business information in motion and at rest ‘important’ to ‘extremely important’
- Half say that their email and SharePoint content is growing at a rate of more than 30 percent annually
- 75 percent indicate that reducing the amount of storage for unstructured information is ‘important’ to ‘extremely important’
- Only 15 percent would ‘bet their paycheck’ that they could quickly produce information required for legal discovery
UNSTRUCTURED INFORMATION: HANDLE WITH CARE

As IT leaders struggle to find smart ways to meet these challenges, many have understandably tried to impose order on their unstructured information at the points of pain. However we believe that this is an operationally hazardous way forward.

Unstructured information – in the form of emails, Instant Messaging (IM) or files – is here to stay. It’s an inevitable result of the powerfully open, flexible and interconnected way we all work, empowering business agility and competitiveness in the global economy.

However the flip side is that information is now at risk everywhere. A new survey of IT leaders reveals that unstructured information is the root cause of a whole range of pressing security and operational challenges, as well as a major driver of rising IT storage costs.*

Soaring information volumes from business-critical applications like email and IM need to be secured and managed on dwindling IT budgets, and incidents of internal data loss are growing alongside external security threats.

Unstructured information is triggering major legal and compliance problems too, not to mention added expense. For most companies today, the cost of recovering and reviewing information is a staggering 1400 times the cost of simply storing it. With companies whose annual revenues top $1 billion fighting an average 556 law suits each year, those cumulative figures are a huge ongoing budget drain.**

There’s also an urgent need to put the brakes on rising data center power and cooling costs and deliver the greener operations that everyone is talking about – but few are yet achieving.

“For Mitel, Information Risk Management started with using the Enterprise Vault family of products to efficiently archive, de-duplicate, and search for email and files for business, legal or regulatory reasons. Partnering with Symantec to secure and manage unstructured information helps us make it easier to leverage the information we want, when we want it, without having to disrupt our business processes, and assuring that we are 100% compliant with legal requirements. Further, the cost savings and efficiency gains are well over $1 million.”

Mark Olsen, Director of Controls And Compliance, Mitel

*Symantec IRM survey September 2008 conducted by Applied Research
**Fullbright & Jaworski, 4th Annual Litigation Trends Survey 2007
Because security, storage and search often manifest themselves in the business as separate challenges, it’s tempting to treat them that way. However this almost always leaves dangerous gaps between solutions and devours IT administration budgets.

Solutions deployed to alleviate issues in one area often end up simply aggravating problems in another – with security solutions hindering the freedom of authorised individuals to search information, to take just one example.

A HOLISTIC APPROACH IS THE KEY

UNTIL NOW, BUSINESS AND IT COMMUNITIES HAVEN’T HAD MUCH CHOICE: POINT SOLUTIONS ARE ALL THAT HAVE BEEN AVAILABLE. BUT THAT’S ALL CHANGING, THANKS TO SYMANTEC’S UNIQUE NEW INFORMATION RISK MANAGEMENT APPROACH.

For the first time, we’re giving IT leaders simple and cost-effective ways to secure, manage and automate control of their unstructured information – now, and in the long term. Our end-to-end strategy protects unstructured information and makes it accessible, wherever it flows or resides, while reducing storage overheads and automating high-cost workflows.

It all starts with a holistic approach towards securing and managing unstructured information: one that keeps attackers out, information in and enables the smart storage and easy search of information. Working this way delivers a number of very welcome added business benefits too, including the ability to:

• Reduce server and storage costs by up to 60%
• Slash the cost and risk of legal discovery
• Reduce the risk of not finding information
• Mine information to improve your competitiveness

What if we also told you that our new Information Risk Management strategy was built on integrated best-of-breed solutions, each one the top-selling solution in its market segment according to Gartner and IDC?

WOULDN’T YOU WANT TO KNOW MORE?

*Gartner Dataquest Insight Email Archiving Software Market 2008 and IDC Worldwide Email Archiving Applications 2008 – 2012 Forecast Update and 2007 Vendor Shares
YOUR FIRST CHALLENGE: PROTECT INFORMATION EVERYWHERE

SECURE UNSTRUCTURED INFORMATION AT EVERY RISK FLASHPOINT

The endpoint is the starting point for risk

Information is at risk on an ever-increasing number of endpoint devices. Portable technologies like mobile phones, laptops and USB data sticks are particularly vulnerable. However tape and disk, email archives, servers and databases are also causing serious security headaches.¹ The growing trend towards outsourcing and contracting puts more and more endpoints outside the direct control of IT departments too, making it even harder to protect against the copying and printing of high-risk information.

But it’s the people who form the perimeter of every business who are the real soft targets, with the number of recorded phishing sites skyrocketing 167 percent from July to December 2007 alone. More worrying still, many of these criminal attacks take advantage of how people share information, with a massive 40 percent of malicious code being spread by file sharing in the same 6 month period.”

EXPENSIVE MISTAKES
THE AVERAGE TOTAL COST OF A DATA BREACH IN 2007 WAS OVER $6 MILLION – WITH THE MAJORITY CAUSED ACCIDENTALLY BY THE LOSS OF A LAPTOP, A SIMPLE ERROR OR POOR ORGANIZATIONAL PROCESS.

From an annual study by the Ponemon Institute:
U.K. Cost of a Data Breach, November 2007

Information in transit
Email volume is expected to grow 50 percent from 2008 – 2012”” as more and more business-critical communication is done over email. Between 2001 and 2008 spam grew from 8 to 80% of all email, with many organizations reporting upwards of 95 percent of email as spam. At the same time, spammers are getting more sophisticated, focusing on profits and criminal activity, and blocking spam is becoming more complicated. Organizations need perimeter protection that prioritizes their legitimate email while starving spammers.

Stored and shared data
Half of IT managers say that their email and Sharepoint content is growing at a rate of more than 30 percent annually.” Ironically, the more precious or controversial a piece of information is, the more places you’re likely to see it copied, stored and transmitted. Putting a complete Information Risk Management strategy in place is the easiest and best way to consistently manage and protect information stored this way on disparate systems: from collaborative technologies like Microsoft Exchange, SharePoint and IBM Lotus Domino to communication systems like IM and everyday file sharing storage.

KEEP ATTACKERS OUT AND INFORMATION IN WITH SYMANTEC’S UNIFIED SECURITY APPROACH

The Symantec Brightmail™ Gateway gives you cost-effective inbound and outbound messaging security for email and IM – delivering powerfully accurate antisamp and antivirus protection, advanced content filtering and data loss prevention. It also protects against new messaging threats and catches over 97% of spam using continuous automatic updates, global and local IP reputation analysis and comprehensive reporting.

This integrates seamlessly with our Symantec Data Loss Prevention solution: the industry’s first to combine endpoint and network-based software to protect confidential data wherever it is stored or used. Layered architecture lets you prevent both malicious and unintentional data breaches whether data is stored on the network or on a disconnected endpoint owned by an outsourcer or employee, and stops data exiting any network gateway or endpoint.

¹ Vontu and Ponemon Institute survey study (August 2006) shows that 4:5 companies lost data on laptops.
² Vontu and Forrester Consulting survey (February 2007) shows that 1:2 companies lost data on USB drive.
INFORMATION OVERLOAD: HOW TO SECURE AND MANAGE IT TO YOUR COMPETITIVE ADVANTAGE

YOUR SECOND CHALLENGE:
REDUCE THE COST OF STORING INFORMATION

STAMP DOWN INFORMATION MANAGEMENT OVERHEAD

Spiralling costs can’t go on
Everyone knows that storing unstructured information is a huge, ongoing budget drain. With storage bills increasing at more than three times the rate of IT budgets according to Gartner,¹ storage is actively siphoning budgets from other critical areas of IT that more directly contribute to company growth and performance.

Storing email almost certainly causes businesses the most pain, and a recent study by The Radicatti group estimated that things are only going to get worse, with email volumes set to increase by 50% from 2006-2010.²

Not all data is created equal
The first secret to reigning in storage costs is to embrace the fact that data is always a mixed bag, including business and personal email and spam. Organization’s need to find automated, repeatable ways to intelligently classify and centrally archive unstructured information – applying retention and expiry rules across different information classes to ensure they keep only what is necessary, only for as long as is necessary.

Automating traditionally manual tasks like data de-duplication and backup also becomes easier once data is centrally stored and managed – meaning that organizations can do more of this laborious and time-consuming work cost-effectively in-house, reducing expensive outsourcing bills.

The result? Leaner, greener IT
Compressing information, cutting index size and actively deleting information that is no longer required lets IT accommodate more users per server and reduce server counts. Lower ongoing costs are matched by lower energy and cooling requirements too – delivering a lower overall carbon footprint.


The fundamental challenge is that a single email can often be stored many times over within an organization: on the email server, on a user’s PC, in a .pst or .nsf file, on file servers and then saved in SharePoint and in backups.

Of course, all this stored information needs to be compressed, and then indexed to make it searchable. However to deliver optimized search speeds and drive smart algorithms, search technologies typically create an index that’s 50-100 percent of the size of the information being searched, obliterating the benefits gained by compression.

The glimmer of good news – that storage costs per bit are falling – is wiped out by rising power, cooling and data center costs too.

REDUCE, REUSE AND RECYCLE WITH SYMANTEC’S UNIFIED STORAGE APPROACH

Symantec Enterprise Vault™ uses compression and single instancing to dramatically reduce storage and control index size: storing just one copy of an item across all logical archives. That means you can slash your storage, power and cooling overheads and use the hardware you already have, much more efficiently.

Smart retention policies let you automatically delete data when it is no longer needed and reuse your storage too. This kind of automated deletion process is also more legally defensible, avoiding the arbitrary, user-driven deletion of information.

Symantec Enterprise Vault also offers the industry’s only direct tape to archive solution – so you can start recycling tapes rather than building a library that just keeps growing.
YOUR THIRD CHALLENGE: AUTOMATE HIGH COST WORKFLOWS

GIVE POWER TO THE PEOPLE WHO REALLY NEED IT

Legal discovery or disclosure: why not help yourself?
Successfully combating legal challenges and keeping litigation costs down often hinges on being able to rapidly assess a case in its early stages. What’s the risk from legal action? Can your company handle the matter itself? Is expensive outside counsel necessary?

Answering these questions and responding to any corporate lawsuit or internal investigation almost always involves collecting and delivering a range of emails, files, instant messages and other data for legal review. Being able to automatically search across one, centralized and intelligently classified archive using simple tools can significantly lower the cost of collecting this data. Applying automated data retention and expiry policies to keep the archive size in check also makes the review and analysis of archived items much quicker and easier, giving lawyers less to request and review.

A MIDSIZE CASE CAN GENERATE UP TO 500 GB OF POTENTIALLY RELEVANT DATA. IT COULD COST AS MUCH AS $3.5 MILLION TO PROCESS AND REVIEW THAT MUCH INFORMATION BEFORE PRODUCTION.
E-Discovery: A view from the Frontlines, 2008, Institute for the Advancement of the American Legal System

Criminal, HR and security investigations
When a criminal investigation is taking place, discovery processes need to preserve a chain of custody for all documents, files and messages. Separate access for information and administration purposes also needs to be set up and the comprehensive forensic capture of any physical material found on laptops, desktops and other endpoints ensured.

This approach can also support HR and security-based investigations with the additional requirement of the careful segregation of searches and granular access rights, as it’s often IT staff themselves who are being investigated.

WHY AUTOMATE?
1GB OF EMAIL BREAKS DOWN INTO ABOUT 100,000 EMAILS. USING A MANUAL PROCESS, AN INDIVIDUAL WOULD NEED TO DECIDE WHAT TO KEEP AND WHAT TO DELETE, EMAIL BY EMAIL. WORKING FLAT OUT, THEY CAN MAKE 10,000 DECISIONS AN HOUR, AT BEST. THAT MEANS IT WILL TAKE 10 HOURS TO DECIDE WHAT TO KEEP AND WHAT TO DELETE IN JUST 1GB OF EMAIL.

Symantec believes that the ideal solution is to offer lawyers, Human Resource (HR) professionals and other investigative teams the self-service tools they need to perform their own searches. This lets organizations dramatically reduce the amount of external counsel they need, freeing in-house legal and HR teams to do the discovery or disclosure work themselves.

This kind of self-service model can help to seriously reduce the high costs often involved in e-discovery workflows, helping professionals:

• Rapidly size up the scope of a problem and choose a course of action
• Locate only the relevant information, at speed
• Do more in-house, slashing the cost of information collection and review
• Effortlessly implement preservation and legal hold requirements

Symantec Enterprise Vault Discovery Accelerator puts a company’s archive in the hands of the legal, HR and investigative teams who need to search it. Self-service discovery tools help them focus on driving investigations and winning legal cases, while freeing up IT to focus on day-to-day network continuity.

By extending the basic search functionality of Enterprise Vault, Symantec Enterprise Vault Discovery Accelerator lowers the cost of data collection. It also preserves relevant archived items in electronic discovery for delivery to any requesting parties, through a highly flexible and audited export process. Authorised personnel are empowered to conduct advanced searches and analysis too: from guided reviews and conversation threading to bulk marking and tagging.

Interfacing with Symantec Enterprise Vault provides businesses with the industry’s only direct connection to attorney review platforms – letting them leverage attorney work products, marks and comments in the archive and access them again in future searches. That means that marks can be re-used, so that repeat reviews don’t need to be conducted at great legal expense.
The team at Symantec is here to help you meet your unstructured information challenges by working within, around and about them: embracing the innovative ways that people share data; adapting to the tools that people choose to use; and enabling staff to work unhindered, in the way they always have.

With our powerfully holistic Information Risk Management approach, you’ll finally be able to both protect unstructured information and make it accessible everywhere, while reducing storage overheads and automating high-cost workflows. And the real beauty is that you can achieve all this without disrupting business as usual.

What it takes is the creation of an exceptionally open and flexible infrastructure. One that delivers end-to-end solutions for security, storage and search challenges – rather than erecting impermeable solutions at the point of pain that create snags in information flow.

Only by tackling security, storage and search challenges all together in this way can organizations achieve a truly robust approach to Information Risk Management. And Symantec is able to help you do this: solving all three interlinked challenges based on a single Symantec Enterprise Vault classification engine, to help you apply policies consistently.

The added advantage of this approach is that you don’t need to force a change in employee behaviour – a move that is usually doomed to failure – or implement expensive new process changes and mass retraining programmes.

And the extra reassurance you enjoy is that all the Symantec solutions discussed in this paper are best-of-breed: each ranked number one in the marketplace by Gartner and IDC.*

Why now?
Economic turbulence is causing an unprecedented operational budget squeeze and regulatory pressures keep on tightening. There’s never been a more urgent need to find more cost-efficient, smarter, future-proof ways of working that will protect the unstructured information that is, after all, the oxygen of your business.

* Gartner Dataquest Insight Email Archiving Software Market 2008 and IDC Worldwide Email Archiving Applications 2008 – 2012 Forecast Update and 2007 Vendor Shares

To discuss the issues raised here and explore your next steps, please contact your Symantec account manager.
Alternatively visit http://go.symantec.com/irm/