

MANAGING RISK IN AN UNCERTAIN WORLD

An IT manager starts off the week with a hardware failure on a server running the firm's CRM application. Sales and marketing, as well as senior management, are flustered – they can't access the application to contact key customers regarding a change to a scheduled product delivery date. The IT manager had a replacement server on hand—a rarity in today's tough financial environment—and was able to get the new hardware up and running quickly. The IT team needed to cut some corners in the interest of time – they decided security checks and data de-duplication efforts could wait. They were able to meet their prescribed recovery time objective, and more importantly, the business managers stopped complaining, so the IT team felt the crisis was resolved positively.

This type of scenario plays out in companies around the world every day; yet, what potential risk has been introduced with the approach the IT team decided to take? IT professionals are increasingly responsible for doing more than just provisioning servers and maintaining applications – they are core players in the risk management process.

“Risk never sleeps” – or so goes the phrase made popular by a recent series of Travelers Insurance advertisements, where a metaphorical character representing risk wanders aimlessly and sleeplessly through a city, followed by a series of humorous mishaps.

The concept may seem simple, but its truth is without question. Today’s businesses face a rapidly evolving threat universe, ranging from fires and floods, to increasingly sophisticated hackers and stolen data, to hardware and software outages.

Risk also extends to accounting errors and fraudulent activity, and in 2002, Sarbanes-Oxley legislation was enacted to help organizations increase transparency and minimize these risks, which had badly shaken the foundation of confidence in the public markets and the U.S. economy.

Recent studies suggest that overall, Sarbanes-Oxley has been successful in boosting corporate governance standards and increasing investor and market confidence. Glass Lewis, an investment advisory firm, points to the fact that in 2006, restatements – revisions of previously released financial statements – at large public companies fell by 14 percent, one piece of proof that Sarbanes-Oxley is improving the accuracy of financial statements.¹

A recent poll by Financial Executives International, an advocacy group for chief financial officers and controllers, echoed these sentiments – with nearly half of all financial executives agreeing that Section 404 has made their financial reports more accurate and reliable.² Section 404 of the Sarbanes-Oxley Act requires companies to report on the internal controls they have in place to ensure ethical conduct related to financial reporting, which the senior management must attest to annually. It is designed to improve the public’s trust and confidence in the financial information that companies report publicly.

However, the cost of compliance can be high, particularly from a business psychology perspective. A recent PricewaterhouseCoopers report suggests that an overriding focus on avoiding risk at all costs often causes organizations to implement layer upon layer of controls in endless pursuit of “zero risk”³ – a fallacy which simply does not exist, by virtue of the fact that many risks (floods, fires and other natural disasters, for example) are completely unpredictable.

Furthermore, Sarbanes-Oxley brings with it its own degree of risk – the risk of non-compliance – which can be quite costly, resulting in hefty fines or even prison sentences for top executives.

Today’s businesses face a rapidly evolving threat universe, ranging from fires and floods, to increasingly sophisticated hackers and stolen data, to hardware and software outages.

Over the years, SunGard has seen organizations make great strides in transforming their views of risk and regulation from a cumbersome, costly challenge, to a valuable framework for increasing transparency and protecting shareholders' interests; asserting greater control over operational risks, known as operational risk management (ORM); and accurately assessing enterprise-wide risk levels in order to drive competitive advantage through more productive use of capital resources.

In the five years post-Sarbanes-Oxley, widely-held attitudes toward risk and regulation may have changed, but one notion that hasn't changed is the need to bring specific operational risk factors – including IT-related risk factors – under control. In business, the term ORM refers to the oversight of many forms of day-to-day operational risks including the risk of loss resulting from inadequate or failed internal processes, people and systems or external events.

Information availability, data privacy and security and information lifecycle management (ILM) have been, and continue to be, three key areas of IT that businesses focus on in order to reduce risk of non-compliance. The primary reason is that these three areas can significantly impact the completeness and validity of financial reports. But these three areas also represent, in and of themselves, operational risks that can exert long-term damage to company reputation and the bottom line if not properly controlled.

While risk can never be eliminated entirely, this white paper explores the new approaches businesses are taking to fortify these IT areas and minimize their risk potential. At times, these approaches involve combining new technologies with a renewed focus on more traditional techniques at the people and planning levels.

INFORMATION AVAILABILITY

It's no wonder that business continuity capabilities (or lack thereof) are consistently viewed as a top risk factor, considering the pure cost of availability lapses in business terms. It's a cost that is difficult to quantify, particularly when factoring in the potential loss of repeat business and tarnished company reputation that may occur after a highly publicized outage.

ABOUT PINGDOM

Pingdom has a very strong and narrow focus which lies in "covering the uptime monitoring needs of 90% of the companies in the world." More specifically, Pingdom monitors and reports on the uptime performance of leading websites supporting a vast majority of the world's online business initiatives, including Yahoo! and Google.

According to Pingdom, "If you are a business with an online presence, it is important that your website and other online services are available 24/7, all year round. However, all websites have occasional problems, whether the reason is external or internal, and there is a significant risk that you are unaware of these problems. Poor online availability can become costly both in terms of lost goodwill and lost business opportunities. The Internet is more and more becoming the main point of contact, and if you are not there to be seen, you become invisible."

In June 2007, the popular social networking site Facebook experienced a period of extended downtime which it blamed on power issues at one of its data centers. The incident ignited the blogosphere, which quickly criticized Facebook for losing its snappiness and reliability and being unable to satisfy the heavy technical demands of personalized services – an issue which had plagued Facebook’s predecessor, Friendster.⁴

In today’s highly connected world, it’s virtually impossible to keep even the briefest period of downtime a secret. Evidence of this can be seen in uptime monitoring companies like Pingdom, whose sole reason for being is to monitor and report publicly on the performance of leading websites supporting customers’ online initiatives (see sidebar previous page). In April 2007, Pingdom publicly released year-to-date downtime records for leading websites: Yahoo! came out on top (with zero minutes of downtime), with Google falling into second place with seven minutes of downtime. However, YouTube.com and Blogger.com – both owned by Google – were called out for experiencing well over four hours of downtime each.⁵

Today’s IT executives bear heavy responsibility for avoiding these risks. Fortunately, advanced information availability approaches are helping IT executives meet this challenge head on and deliver uninterrupted access to information, which serves to mitigate risk, protect the bottom line and enhance competitive position. Following are examples of the shift from the old, traditional way, to new data recovery and availability methods.

The traditional focus on “always being ready” is evolving to “always being on.”

An “always being ready” approach emphasizes an organization’s ability to recover from a disaster once it has happened or is imminent. In this scenario, the process of getting a business back up and running can take hours or even days – resulting in potentially significant revenue losses.

Conversely, an “always being on” approach helps ensure that organizations have access to data, when and where they need it, depending on the level of criticality as defined by users. For example, truly mission-critical applications would continue processing during an event and resulting data would be captured, thus protecting revenue streams. This can be achieved through application or disk mirroring, or by moving to a managed services model, whereby lifeblood corporate applications and data are operated and housed securely by a third-party specialist at a remote data center location.

The traditional practice of relying solely on tapes for back-up has evolved to supplementing tapes with e-vaulting and/or storage and server replication.

Disasters can damage tapes, or prevent tapes from getting to their desired locations in a timely fashion altogether. Sole reliance on tapes that may not be properly stored or transported can also increase vulnerability to tape loss or theft.

By supplementing tapes with e-vaulting (electronic back-up to a remote location, such as a disk array at an off-site data center managed by a third party), businesses can help ensure continuous automated back-up to a secure site – for their most critical and sensitive data – driving a higher level of data availability, security and continuity.

Real-time storage replication (copying or mirroring data from a source to a target) and server replication (implementing fail-over database servers to pick up processing loads should an interruption occur) allow organizations to reduce recovery time objectives

(RTOs) to a few hours or even a few minutes, and minimize data loss and application recovery time. These techniques are finding favor as quick, reliable solutions for organizations that need to keep information up-to-the-minute. They are also important for databases, email and file servers, where extended downtime may represent an unacceptable business risk.

The traditional focus on driving greater data center resiliency has expanded to include partners and customers.

Rapidly proliferating collaborative networks require businesses to be able to communicate outside their four walls to maintain 24/7 access to customers and partners. Businesses are deploying network recovery solutions to achieve “always on” connectivity for their network, website and IP connections, through global, protocol-independent, resilient networks designed to meet needs for fast and reliable recovery.

However, new risks such as that of an avian flu pandemic could potentially take down or disrupt the public Internet altogether, as more employees work from home and networks become overloaded. Today’s IT executives are collaborating with third-party experts to architect plans to ensure that their most critical employees maintain network access – even if it means limited access for other employees, temporarily.

However, the more things change, the more certain elements must stay the same.

The industry has gone through significant leaps and bounds to reduce business continuity-related risks. The new information availability approaches described above have had a positive impact, but an Achilles heel of many organizations is the tendency to focus on the latest and greatest technology without paying due attention to the equally critical components of people, processes and planning. In fact, as technology grows more complex and advanced, there’s an even greater likelihood that organizations won’t pay enough attention to these elements because they erroneously think that technology has the job covered.

As many are all too painfully aware, IT disruptions are an unpredictable element of risk and reinforce the notion of “zero risk” as a fallacy. However, this does not mean that organizations are completely at the mercy of these risks. Organizations need a strong focus on three core elements – people, processes and planning – coupled with decisive leadership, in addition to technology. This is a “back to basics” approach to information availability which further fortifies an organization against unplanned risks coming in the form of disasters or other unexpected events. For example:

PEOPLE ARE THE HEARTBEAT OF THE ORGANIZATION:

No matter how advanced an organization’s technology may be, it’s the employees who are at the core of a company, because they are the ones to recover the environment and resume business processes at the time of a disruption. To illustrate this point, an organization that has 100 percent of its data fully replicated and running at a hot site will remain paralyzed if it doesn’t have the right people there who are trained and equipped to take the reins and bring the organization back onto its feet.

Companies need to ensure the right people are available to execute business recovery processes, based on preplanned guidance and scenarios. They must also plan for the possibility that lower level staff may have to make critical decisions due to a lack of executive team availability. This requires an understanding of who represents the organization’s “brain trust” during the normal course of business, and establishing a “back-up chain of command.” Those representing the brain trust must then prepare their respective “back-ups” in the chain to make decisions in their absence.

A focus on people also requires an organization to comprehensively consider and document a wide range of processes and issues including:

- What is the chain of command? That is, who decides what, and when?
- Where are the people going if the building is unavailable?
- Who's going, and who determines who is making the trip?
- How are they going to get there?
- How long are they going to stay there?
- If this is a long-term scenario, what about their families?

Processes and documentation: When a disaster strikes there are three major steps to begin the process of managing the incident:

1. mobilizing a central command center;
2. activating a business recovery plan; and
3. identifying exactly how long the organization will operate in a recovery state, and planning accordingly.

Should a potentially disruptive event of any kind occur, the fact that many employees would not be aware of an overall business continuity plan – or their roles within such a plan – is alarming, to say the least.

Following closely behind the imperative of managing people is the need for organizations to carefully document their processes, both in terms of how to recover and how to operate. Organizations also need to practice and refine processes using a variety of scenarios.

For example, if a central command center becomes unavailable due to a natural disaster, where is the default command center? What applications and systems should be brought online first, and in what order? Does this answer vary based on the nature of the business disruption? What level of damage to an organization's primary site warrants a complete move to a new site? At what point are conditions considered safe or stable enough for employees to report back to the primary site, and what is the proper process for communicating this throughout the organization?

Planning, communicating and practicing the information availability plan: Once processes are established and documented, the next critical step is to effectively communicate these processes to employees and thoroughly practice the actual execution of the process parameters, or the business continuity plan.

Communications is one area where many organizations are falling very short.

According to a recent IDG Research⁶ survey, almost half (44 percent) of respondents indicated their organizations never communicate an overall business continuity plan to employees. Fifty-nine percent go on to state their organizations do not articulate their organization's business continuity plan to key external stakeholders.

Should a potentially disruptive event of any kind occur, the fact that many employees would not be aware of an overall business continuity plan – or their roles within such a plan – is alarming, to say the least.

These responses also seem at odds with heightened expectations for greater corporate transparency and communications on the part of all critical stakeholders, extending beyond employees to partners, customers and shareholders. Stakeholders should expect a comprehensive picture of how their organizations would respond to a business disruption, as a means of holistically understanding their

own risk and adopting precautionary, self-protective measures when needed. Here, again, the need for leadership becomes apparent. A commitment to business resiliency that is continually communicated at the highest levels of an organization reinforces a perception that the organization is in good hands and “knows what it is doing.”

Finally, the importance of testing and conducting disaster recovery dry-runs cannot be over-estimated. IDG Research also uncovered an alarming percentage of respondents whose companies do not test their plans often enough for them to be most effective during a disruption. A total of 80% indicated they test their disaster recovery plans annually or less often.⁷

In the past, annual testing may have been sufficient to accommodate changes in business processes; however, today, organizations are facing ever-increasing, nearly constant (and sometimes daily) changes to mission-critical processes and systems, from staff updates to alterations in hardware and software. As a result, business continuity plans become outdated much more quickly than in the past. An organization that tests its plans once a year – or less often – may be able to recover, but the road to recovery is apt to be longer and riddled with speed bumps that can take their toll on business resumption and corporate reputation.

DATA PRIVACY AND SECURITY

In the quest for greater efficiency, businesses worldwide have looked to increase data accessibility via back-up tapes, computers, networks, the Internet and wireless devices. But unless properly managed, increased accessibility can also mean greater vulnerability to risk in the form of mishandled or stolen data, or unplanned downtime as a result of malicious network activity. Vulnerability to these risks increases every time a new system, user or device is added to the network.

In spite of this challenge, it remains the fundamental responsibility of businesses to secure customer and corporate information to minimize this potential risk. Criminal activity involving the information technology infrastructure is a rapidly growing concern for the global community. The FBI now ranks cybercrime as its third priority behind terrorism and espionage. McAfee CEO David DeWalt recently noted that cybercrime – which has become a \$105 billion business – now surpasses the value of the illegal drug trade worldwide.⁸

Since the advent of the Internet, there have been dozens of widely publicized security breaches and incidents that have heightened the risk of lost customer confidence and trust for the companies involved. For example:

- In January 2007, TJX Corporation, a Framingham, Massachusetts-based retailer which owns brands such as TJ Maxx, Marshall’s and Bob’s Stores, reported that unknown intruders had accessed its payments systems and account data belonging to an unknown number of customers in multiple countries. At the time, TJX said it believed the intrusion took place in May 2006, even though it didn’t discover the breach until mid-December 2006. A few weeks later, the company revealed the intrusion actually took place in July 2005. Casting further doubt and uncertainty, TJX had originally reported that data from 45.6 million payment cards had been exposed, but in October 2007, reports showed that the actual number may have been as high as 94 million.⁹

Since January 2007, the TJX breach has prompted several lawsuits and investigations by the Federal Trade Commission and the attorneys general of several states as well as numerous class action lawsuits. It has also spurred a hefty dose of negative attention from consumer advocacy groups. Not only do the after-effects of the incident continue to linger, but they continue to impose heavy costs – both from a financial and customer confidence perspective.

- In February 2007, Johns Hopkins – a Maryland-based organization comprising Johns Hopkins University and Johns Hopkins Hospital – disclosed that it had lost personal data on roughly 52,000 employees and 83,000 patients in a tape mishap. More specifically, nine tapes containing sensitive information, which were dispatched to a contractor for back-up, were never returned to Johns Hopkins. Both the contractor and Johns Hopkins investigated the incident and reportedly determined that the tapes never reached the facility. “It is highly likely that the tapes were mistakenly left by a courier company hired by the contractor at another stop,” noted a statement on the Johns Hopkins website.

While the tapes were thought to have been incinerated, Johns Hopkins was forced to notify all employees – current and former – as well as all patients, and undertake an exhaustive review of processes and procedures. The Johns Hopkins example illustrates the danger and high costs of human error often associated with transporting and storing back-up tapes.

- In September 2007, online brokerage TD Ameritrade Holding Corp. (Ameritrade) announced that a hacker broke into one of its databases and stole personally identifying information for some of its 6.3 million customers. An online advisory and letters to account holders disclosed that names, email addresses, phone numbers and home addresses were taken in the data breach. While clients’ financial assets were never touched, affected customers did experience a highly annoying and inconvenient increase in spam, resulting in a public apology from Ameritrade’s management.

AVAILABILITY AND SECURITY: DICHOTOMOUS ENDS?

Therein lies the fundamental challenge for today’s organizations – how to guarantee information availability combined with privacy and security. Companies are now minimizing information privacy and security risks through comprehensive security programs comprising professional information security consulting services and managed security services. This approach provides ideal protection against a treacherous and dynamic threat environment.

Where security is concerned, consultants need to do more than provide standard recommendations and uniform best practices for technology applications. Rather, they need to take into account each organization’s unique data security priorities and most vulnerable points of weakness in order to design and implement tailored, effective solutions.

This professional consulting services approach follows four main steps:

- **Prioritization of systems and applications** – Understanding that many organizations have limited resources, professional services consultants should conduct a comprehensive audit with the organization to segregate and prioritize which systems need to be most available and secure. For instance, a business may deem its credit card transaction processing systems as the most critical and align resources accordingly, while a procurement system for non-critical supplies – pens and paper, for example – can afford a bit more leniency. Classifying data this way offers cost savings allowing important (but not mission-critical) data to live on lower-cost storage options.
- **Enterprise risk assessment** – Once systems and applications are prioritized, a consultant conducts a comprehensive enterprise risk assessment focused on the applications and systems that need to be most secure, as well as common threats to overall data security. For a typical enterprise, these threats may include hacking, fraud or identity theft, denial-of-service attacks, malware or spyware. The consultant must demonstrate an understanding of the unique characteristics of the broadest possible range of threats, in order to gauge threat-by-threat risk levels and formulate an accurate overall risk assessment. The practice of measuring against ISO 17799 – the industry data security standard – helps establish a performance benchmark.

- **Information availability assessment** – Professional consultants must also understand and convey how this overall risk assessment affects information availability, and the resulting implications that must factor into business decisions. For example, if risk is considered sizeable, resource allocations that otherwise would have gone toward a more strategic investment – for instance, opening new locations and/or expanding into new markets – may have to be set aside in order to cover the potential cost of the organization being down or not operating properly for a certain period of time. Simultaneously, this assessment will influence technology decisions (e.g., implementing server replication as a means of reducing the risk of data loss in the event of a disruption).
- **Ongoing testing** – Consultants should put a program in place to simulate aggressive network attacks as a gauge of real resistance levels. Aggressive testing should not be considered a one-time event, but rather, an ongoing, regular procedure that addresses and adapts to the constantly evolving security landscape.

Looking beyond professional services, a managed security services approach provides ongoing, reliable protection against a wide variety of threats. Other key benefits include the ability to offload relatively mundane tasks such as access management, freeing up IT staff to focus on more strategic, revenue-generating and/or customer-focused initiatives. In addition, from the perspective of ongoing cost and continuity of delivery, there are tremendous benefits from leveraging dedicated third-party experts equipped with the industry's most current tools and technologies in the following areas:

- **Firewall and VPN services** – Known as the first layer of protection, managed firewall services provide round-the-clock protection against intrusions, while managed services configure a VPN to provide remote users with reliable access to the systems and data they need.
- **Intrusion detection and prevention** – By extending firewall capabilities, this service leverages intelligent sensors to check traffic for malicious activities coming from internal or external sources. When the service detects suspicious events – ranging from protocol violations and suspect traffic patterns to repeated login failures – it immediately alerts network administrators. If configured in its prevention mode, the service can also block the events before they affect systems or networks.
- **Vulnerability protection** – Using an advanced scanning technology, this service automatically scans for network security weaknesses on firewalls, Web, FTP and DNS servers, routers and other systems. The service also examines networks on a regular basis to locate potential weak points and suggest strategies to fix them.
- **Identity and access management** – Identity and access management services help organizations configure and manage user access and authorization.
- **New portal offerings** – These provide a first-hand view – at any point in time – into the real-time performance of managed services.

As a final note, combining consulting and managed services drives maximum impact through greater collaboration and knowledge-sharing. For example, consultants may work with an organization to define policy procedures – such as optimal password complexity and duration for a particular application – based on the value of the inherent information. Managed services can then tailor and deliver identity and access management services in a manner supporting the defined policies.

INFORMATION LIFECYCLE MANAGEMENT

Information lifecycle management (ILM) is a comprehensive approach to managing the flow of an information system's data and associated metadata, from creation and initial storage to the time when it becomes obsolete and is deleted. ILM has become increasingly important as businesses face compliance issues in the wake of legislation like Sarbanes-Oxley, which dictates how organizations must deal with particular types of data.

Sarbanes-Oxley is not a set of business practices and does not specify how a business should store records; rather, it defines which records are to be stored and for how long. For this reason, the legislation not only affects the financial side of corporations, but also the IT department whose job it is to store a corporation's electronic records and documents.

For example, Sarbanes-Oxley states that all business records, including electronic records and electronic messages, must be saved for "not less than five years."

This is no easy task, given that email use (see sidebar) and corresponding storage requirements are growing at a rampant pace across the business world. Gartner estimates that the worldwide e-mail active-archiving market was \$376 million in new software license revenue and maintenance services in 2007, an increase of 33.7% over 2006. The market is expected to grow to \$1.7 billion by 2012.¹²

Newer legislation like e-Discovery, enacted in 2006, places further strain on IT departments in that instant messages – an increasingly popular form of business communications – must be archived in the same comprehensive manner as email (see sidebar). In its Third Annual Litigation Trends Survey presented in 2006, the law firm Fulbright & Jaworski LLP found 80 percent of respondents reporting that they were not prepared or only somewhat prepared for e-discovery.

The survey also revealed that the average company with more than \$1 billion in annual revenue is currently facing more than 500 discrete lawsuits where that company must produce email messages. The cost to retrieve and review the messages can be as much as \$2 per message and can total more than \$30 million in annual legal expenditures.¹³

Regardless, failure to comply with ILM requirements put forth by Sarbanes-Oxley and e-Discovery can be costly – resulting in heavy fines, sanctions or even prison sentences. IT departments therefore face tremendous pressure to create and maintain a corporate records archive in a cost-effective fashion that satisfies the requirements put forth by legislation.

EXPLOSIVE GROWTH IN ELECTRONIC MESSAGING

The Radicati Group, a market research firm specializing in messaging, recently reported that the number of active email mailboxes worldwide will jump from 1.4 billion in 2006 to 2.5 billion in 2010.

The number of worldwide instant messaging accounts will increase from 944 million to 1.4 billion in the same time period, while the average daily email storage needs of a corporate email user will increase from 16.4 megabytes to 21.4 megabytes.

However, it is the newer breed of email technologies, like wireless email, that pose the biggest challenge: the number of wireless email users is expected to increase from 14 million in 2006 to 228 million in 2010. The reason for this may be that the majority of people have email and instant messaging accounts already, while there is still plenty of room for more wireless email users, since this is still a fairly new activity for most people.¹⁰

In doing so, IT departments must also ensure that data is saved in a manner that does not slow or impede data recovery efforts and/or access to the most critical corporate data in the event of a business disruption.

Today, many organizations are looking to managed email archiving solutions to deliver highly reliable email retention, availability and management designed to address specific regulatory, business and technical needs. The services provide a secure and reliable way to capture, transmit, archive, store and retrieve emails while helping meet compliance requirements. The services also help organizations to optimize server performance and reduce email message volume substantially. Lastly, by delivering policy-based email retention and e-discovery with full end-user access and outage protection in a highly cost-effective manner, the services help free up IT resources to manage core business competencies.

WHAT YOU CAN DO TO KEEP PACE WITH RISK – THREE KEY IT AREAS TO FORTIFY

Let's face it, risk may never be eliminated entirely, but there are three key IT areas that if better fortified – information availability, data privacy and security, and information lifecycle management – can help you in your quest to avoid operational risk.

1. Information Availability

Risk management and business continuity go hand-in-hand. Keeping pace with risk means keeping pace with new paradigms for information availability:

- "Always being ready" won't cut it – you must work to be "always on."
- For true back-up, add storage and server replication to your basic tape solution.
- Don't forget the people, processes and IT systems in your planning.

2. Data Privacy and Security

Faster networks, handheld devices, remote working arrangements – these add to our productivity and efficiency, but also infuse opportunities for risk in the enterprise.

E-DISCOVERY

In 2006, the U.S. Supreme Court made several amendments to the Federal Rules of Civil Procedure calling for the rapid and efficient rendering of data evidence in electronic form.

Today, these requirements are known as electronic discovery, or "e-discovery." According to the terms of e-discovery, parties in a lawsuit can now demand from each other word processing documents, emails, voice mail and instant messages, blogs, backup tapes and database files.

This was the first time that emails and instant message chats were designated as likely records that needed to be archived in accordance with a company's records retention policy and produced when relevant. The rapid adoption of instant messaging as a business communications medium during the period 2005-2007 has made instant messaging as ubiquitous in the workplace as email, and created the need for companies to address archiving and retrieval of instant messaging chats to the same extent they do for email.¹¹

Today, organizations that fail to meet e-discovery requirements may find themselves subject to serious sanctions and fines, to the tune of millions of dollars. Or, they may find themselves having to pay staggering fees for the legal manpower needed to sift through thousands of paper-based documents.

When it comes to security, every company is different. To avoid risk, you must consider your unique data security priorities and points of weakness.

Make sure to follow these four steps:

- a) Prioritize your systems and applications
- b) Conduct an enterprise risk assessment
- c) Go through an information availability assessment
- d) Test, test and test again!

3. Information Lifecycle Management

Information lifecycle management has become increasingly important as businesses face compliance issues in the wake of legislation like Sarbanes-Oxley.

ILM can be overwhelming, and presents one of the greatest opportunities for risk. Handing even one aspect to a partner – such as managed email archiving – can help in your efforts to address specific regulatory, business and technical needs.

CONCLUSION

Taking a holistic approach to business continuity, information privacy and security and ILM, with the goal of mitigating operational risk, is no small task. Yet, organizations that are better able to accurately assess and manage operational risk are apt to achieve strategic competitive advantage in their respective marketplaces, combined with stronger public perception.

Often, organizations benefit from expert, third-party assistance. When seeking a partner, organizations should consider firms that offer extensive experience in the three separate areas: information availability, data privacy and security and ILM. It is also helpful to engage a partner that has demonstrated skill in identifying, adopting and deriving best practices from industry rules and regulations.

Working with a partner such as SunGard Availability Services provides a comprehensive enterprise perspective: the peace of mind that comes from working with a trusted partner and third-party objectivity in developing best practices that address multiple regulatory concerns.

SunGard can help develop an overarching and enterprise-wide approach to risk mitigation and incident planning as they relate to corporate governance. SunGard offers a complete array of services to help organizations assess risks; integrate their business continuity, information privacy and security and ILM plans; and continually test and improve consolidated plans and implement them with an eye toward improved risk management, regulatory compliance and controlling costs.

SunGard's team of experts help eliminate identified concerns through targeted risk mitigation services, which address such issues as policies and procedures, architecture, internal controls, monitoring and measuring and awareness.

In short, SunGard helps clients elevate their thinking and plans and drive improved operational and business performance as a positive outcome of risk and regulation.

AUTHORS

This white paper is based on the collective experience of SunGard Availability Services and was written by:
Jim Grogan, MS, CISM, Vice President, Consulting Product Development

REFERENCES

1. Glass Lewis referenced in "Sarbox Controversial, But Seen Doing the Job." Investor's Business Daily. 17 August 2007.
2. Financial Executives International, referenced in "Sarbox Controversial, But Seen Doing the Job." Investor's Business Daily. 17 August 2007.
3. PricewaterhouseCoopers. "Making Smarter Risk Decisions." October 2007.
4. Nick Denton quoted in "Downtime: Facebook Crashes." Valleywag: Silicon Valley's Tech Gossip Rag. 25 May 2007.
5. Royal: The Official Blog of Pingdom. "Downtime in 2007 for the 20 Most Popular Websites." 2 April 2007.
6. IDG Research. "Business Continuity: How to Raise the Bar 2007." 17 July 2007.
7. IDG Research. "Business Continuity: How to Raise the Bar 2007." 17 July 2007.
8. David DeWalt, McAfee, Inc., quoted in "Cyberthreats Outpace Security Measures." InformationWeek. 18 September 2007.
9. Jaikumar Vijayan. "Scope of TJX Data Breach Doubles: 94M Cards Now Said to be Affected." Computerworld. 24 October 2007.
10. The Radicati Group, referenced in "Fun Facts About Email." GigaOM. 12 June 2006.
11. Wikipedia. "Electronic Discovery." 4 October 2007.
12. "Magic Quadrant for E-Mail Active Archiving." 20 May 2008.
13. Fulbright & Jaworski LLP. "The Third Annual Litigation Trends Survey Findings." December 2006.

www.sungardas.com

SunGard Availability Services

680 East Swedesford Road

Wayne, PA 19087

Tel: 800-468-7483

©2010 SunGard. WPS-016

Trademark information: SunGard and the SunGard logo are trademarks or registered trademarks of SunGard Data Systems Inc. or its subsidiaries in the U.S. and other countries. All other trade names are trademarks or registered trademarks of their respective holders.