White Paper

SurfControl®

7 Tips to Enforcing Corporate Governance Policy on your Network

The World's #1 Web & E-mail Filtering Company

7 Tips to Enforcing Corporate Governance Policy on your Network

What has been called a perfect regulatory storm is breaking over your networks. Those networks, indispensable engines of productivity, are now being seen by upper-level management as generators of liability in the wake of new government regulations mandating records retention and production, privacy protection and massive auditing changes.

At the executive level, compliance with the regulations, passed in the wake of management scandals at Enron, WorldCom, Italy's Parmalat food chain and other corporations, is prompting wholesale changes in policy under the rubric of "corporate governance." At the network level, compliance will be reflected in large-scale changes to limit liability — primarily a lack of control of the content on your networks.

More importantly, corporate governance will have boards — and shareholders — scrutinizing productivity and return on investment (ROI). Given that Fortune 1000 companies spent $2.5 Billion in IT upgrades to comply with the Sarbanes-Oxley Act, the primary financial corporate governance law, last year alone,[1] they will expect as an ROI both compliance and productivity; auditability and efficient use of network resources.

Top executives are being required by the Securities and Exchange Commission and other regulators to certify the effectiveness of their business processes, under penalty of jail and heavy fines. They must, in essence, certify that your network policy, design and processes are capable of meeting government requirements in addition to resisting more-familiar security threats and providing efficient services. They will hold network designers, engineers and administrators responsible for implementing compliance projects in a way that protects the company. If the CEO's job is on the line, you can bet yours is. You will have to know what is on your network, and what shouldn't be, in real time.

The new focus on corporate governance will be created in different ways by different companies, although at all, it will begin with the board of directors and top management. Large corporations are already adding chief compliance officers (CCOs), such as David Farrell, recently appointed to that post at Sun Microsystems.[2] The federal government, under the 2002 Federal Information Security Management Act (FISMA) requires its agencies to assign a senior agency information-security officer.

[1] AMR Research, "CIOs: There Is a Sarbanes-Oxley Project in Your Future--Do You Know What It Is?" – By Lindsey Sodano and John Hagerty, AMR Research, 5/6/2003.

[2] *Compliance Week*, "Q&A With Sun Chief Compliance Officer David Farrell," 12/9/2003

At most companies, details of the policies will be worked out between legal and human-resources departments. It will be your job to implement those parts affecting the company network.

To network administrators already burdened with traditional physical and logical security, enforcing corporate governance on the network may seem overwhelming. SurfControl, the world's #1 web and e-mail filtering company provides the following seven tips to help cut through the tangle of policies governing content management:

1. Have an Acceptable Use Policy in writing and ensure it is communicated to all employees.

An Acceptable Use Policy (AUP) is the first line of defense in managing content on your network. That content is generated by employees, who need clear guidance on what is permissible on your systems. An AUP is proactive; in itself, it will to some degree regulate the flow of content onto and off the network once employees understand its requirements.

Most companies have crafted AUPs, prompted by the threat of hostile-workplace-environment lawsuits or simply to minimize unproductive network use. New corporate-governance initiatives will require the addition of language detailing the handling of confidential documents, responsibility for auditing- or subpoena-sensitive records and who has the authority to access different classes of content.

AUPs must cover regulations appropriate for your business. Most regulations are about keeping private data private, such as financial records, patient records or company financials. Compliance with those regulations, and confidentiality of industry-specific data, is the responsibility of the entire organization and can be enforced within IT.

Regulators and lawyers have made it clear that AUPs provide corporate protection only if they have been provably communicated to all employees. AUPs should be integrated with other mandated employee training and documented by human-resources departments. In drafting and distributing AUPs, IT needs to work closely with HR, a fact highlighted in a recent report by AMR Research. You must be able to prove that employees actually *read* your AUP, for example.

"Being able to prove that employees attended training sessions … is more important than showing that you offered the training class," writes AMR's Monica Barron. "Make sure you have processes and systems in place to deliver *and* track training history for current and new employees."[3]

[3] Ibid.

SurfControl provides more resources on creating an AUP at:
http://www.surfcontrol.com/resources/aup/

2. The IT department must thoroughly understand policy to ensure accurate and appropriate execution.

At some point, policy has to evolve into a set of practices standard enough for implementation by IT departments. The process of crafting network operating standards will likely begin with the CIO/CTO and, in companies large enough to have them, the chief information-security officer (CISO), but all of IT should be involved as much as possible, so that policy will translate into best practices, which requires policy understanding at all levels.

The more specific policy is, the more easily you can interpret it into network behavior, especially if the company and regulatory reasons behind the policy have been explained to you.

Your corporate execs will probably not be reinventing the wheel. There are outside sources they will probably draw on in crafting a set of network practices compatible with top-down policy.

Many of these sources are security standards. Execs have policy. Techies have standards.

The "standard" joke is that the nice thing about standards is that there are so many to choose from. If, however, you are trained in policy and the reasons various standards are chosen, you will be better equipped to craft a network that enforces good governance.

Two primary guidelines can be the ISO 17799 information-security standard[4], crafted by the International Organization for Standardization, best known for its ISO 9000 quality-assurance standard, and FISMA[5], written to set a security baseline for government agencies.

The ISO 17799 standard comprises 10 sections, the most relevant to corporate governance being security policy, computer & operations management, system development and maintenance, compliance, security organization and business-continuity management. What ISO 17799 lacks in matching regulatory requirements, it makes up in specificity — The Business Software Alliance, dryly refers to it as "overly detailed for CEO consumption."[6]

[4] The ISO 17799 Directory, http://www.iso-17799.com/
Also, the 71-page standard can be purchased from http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=

[5] The Federal Computer Incident Response Center, http://www.fedcirc.gov/library/legislation/FISMA.html

[6] "Information Security Governance: Toward a Framework for Action," Business Software Alliance, 2003, p. 3.

FISMA is government-, rather than corporate-centric, but is a good example of delineation of security responsibility throughout an IT organization.[7] Data classifications, organized by security goal and the potential impact of security breaches, can be found in Special Publication 800-60, available since Dec. 19, 2003 from the National Institute for Standards and Technology[8]

Whatever sources your company draws on for mating top-down policy with network design and practices, all levels of IT employees should be involved — at least, in verifiable training in policy and procedures; at best, in working with management to ensure that general policy is implementable in the context of network reality.

3. Ensure that employee Web activity is business related.

Any corporate-governance policy encompassing IT must take account of employee Web surfing. A spate of hostile-workplace-environment lawsuits has made companies aware of the liability inherent in workplace-downloaded pornography, sites containing hate content and the like. Many companies, however, are just realizing the potential loss of productivity resulting from even harmless Web-surfing, such as visiting news sites. Estimates show that 20 minutes a day of personal surfing or e-mailing can cost a company with 100 employees more than $8,000 per week. (At $50 per hour per employee.)

SurfControl's experience in the Web content-filtering segment suggests the following techniques for managing Web content entering your network:

1. Blacklist sites that contain content inappropriate for, or irrelevant to, the work of your company. SurfControl's Web filter, for example, operates from a database of more than 6 million sites, containing more than 1.2 billion Web pages.

2. Whitelist sites that are relevant to your company's business, ensuring employee access to needed information. Set up company-specific lists of allowable sites, avoiding false negatives in the filtering process.

3. Set policies to block less-than obvious Web content that sap productivity. Sex, drugs and rock & roll are only a fraction of those that employees visit every day. A recent IDC/SurfControl study found significant traffic to sites offering Internet shopping, online stock trading,

[7] See the NIST's FISMA Implementation Project, http://csrc.nist.gov/sec-cert/

[8] "Guide for Mapping Types of Information and Information Systems to Security Categories," draft, NIST, http://csrc.nist.gov/publications/drafts.html

auction bidding and selling, online games, streaming media, MP3s, and even searching for outside employment.[9] Avoid a brain drain by employees job-hunting on the job.

4. Remember that content can go out, as well as come in, through the Web. Web-mail services, bulletin boards and other Port 80 traffic can be used to send content for which a company can be liable. In the new regulatory environment, outgoing traffic can carry confidential company content or client/patient records protected by privacy law.

As with all traffic, employees should be notified as to what type of Web use is, or isn't, acceptable under company policy. Many employees do not even realize that Web traffic and e-mail messages from work are, under most court decisions, company, rather than personal, property.

4. Establish rules to manage employees' e-mail communications and the company's data.

From a corporate-governance standpoint, this is perhaps the most critical aspect of basic network policy as well as compliance projects. Rules should foremost meet the policy requirements of your specific business in balancing the security and availability of data. To do so, you have to determine, and enforce, the security needs of different types of data, whatever its source: word-processing documents, e-mail, instant messaging or the like.

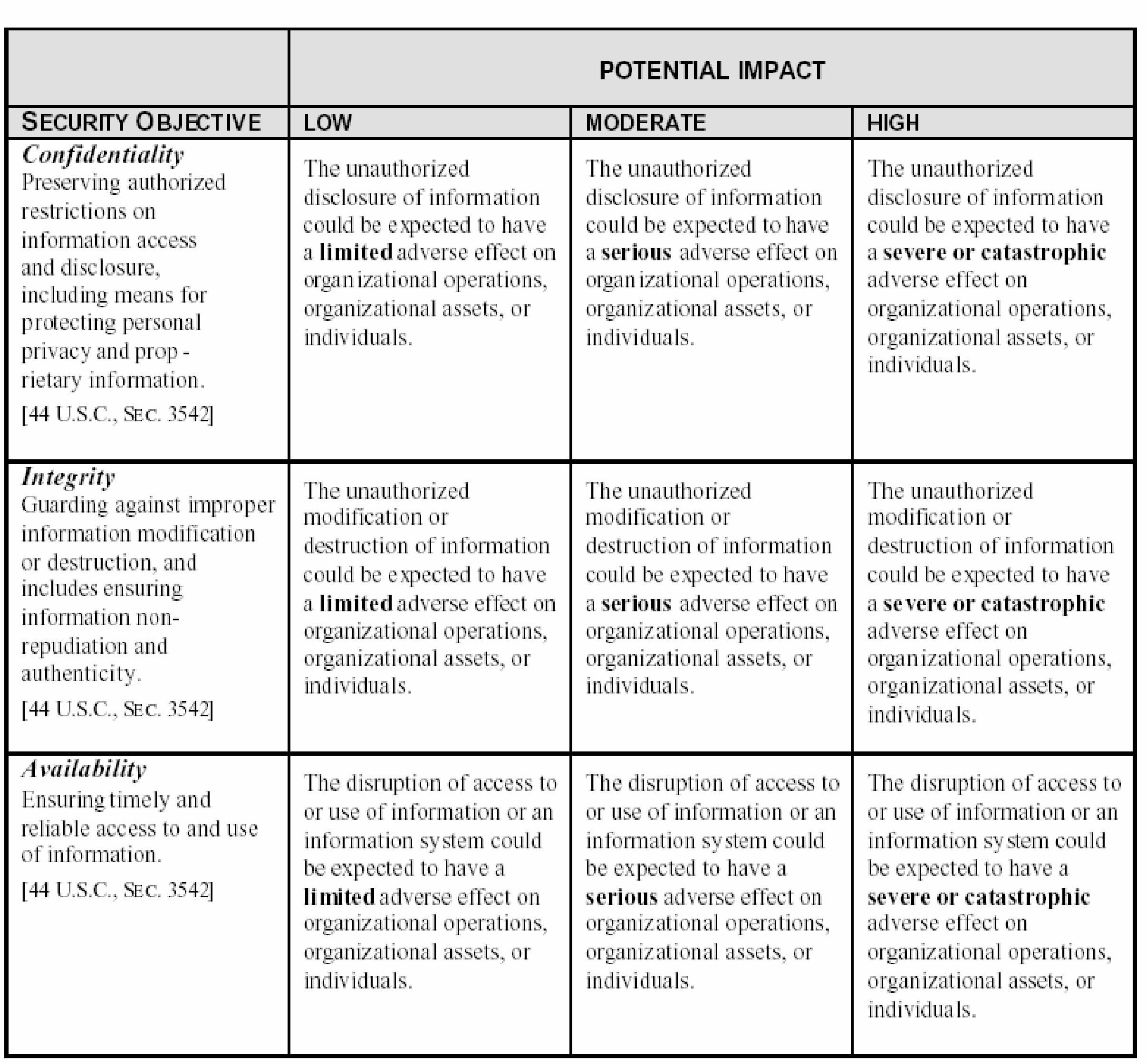
The emergence of e-mail as the primary means of communication within companies, and between employees and the outside world, makes it the primary source of liability. Any slip of the "send" button and confidential data can be lost, creating regulatory breaches. Possible nightmares include making financial announcements too soon, asking a question about a patient to someone who does not have legal access to that patient's records violates HIPAA and sharing mortgage applications between departments in a way that violates the Gramm-Leach-Bliley Act or the Fair Credit Reporting Act.

Here, as elsewhere, the needs of good company security coincide with those of regulatory compliance. According to SC Magazine (Aug. 2001), 90% of any company's intellectual capital, its inventions or source code, for example, is in digital format. Of that, 45% is stored in the organization's e-mail system at any given time. There is too much room for error if proper authorizations and polices are not set at the network level. This requires classifying your e-mail and other data based on its content.

[9] IDC/SurfControl, "Content Security: The Business Value of Blocking Unwanted Content," Brian E. Burke, July 2003.

The NIST's (National Institute of Standards and Technology) SP 800-60, for example, establishes classifications based on the confidentiality, integrity, and availability of data, then defines impact levels of security breaches. In a high-impact breach, for example, "The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals,"[10] according to the NIST.

The final step, and the one that might determine how you would set your data policies, is assigning to security breaches different levels of impact based on particular data's confidentiality, integrity and availability. The following chart shows how security breaches are classified:[11]



	POTENTIAL IMPACT		
SECURITY OBJECTIVE	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

[10] SP 800-60, p. 5.

[11] Ibid., p. 10.

Once the basic data-security needs of the company are defined, they must be merged with the requirements of regulatory compliance.

New SEC regulations are a mailserver admin's nightmare; they require the retention of different types of records for different periods — three years for some; six years, three in an accessible place, for others; yet different periods for other types. Mass archiving and storage is one way to deal with records retention — but it is neither precise nor conducive to rapid production under government pressure.

What most companies don't realize is that not *all* e-mails are necessarily company records — a point the SEC has made clear. "With respect to memoranda, including e-mail messages," the SEC said in its final Books and Records Rule, "the commission has stated that the *content and audience* of the message determine whether a copy must be preserved, regardless of whether the message was sent on paper or sent electronically" (our italics). Monitoring the content and audience of e-mail — a capability every company should have for basic management — is a huge aid to compliance.

Regulators who arrive *en masse* for an inspection can throw an IT department into an uproar, demanding e-mails containing a particular type of content, or to or from particular employees.

Spam remains a growing threat. A new federal anti-spam law, which took effect Jan. 1, is showing no signs of effectiveness, according to the *Washington Post*. "Spam-filtering companies and Internet providers report little change in spam patterns," the *Post* reported Jan. 6, 2004. "Estimates vary, but spam accounts for roughly 60 percent of all e-mail traffic, with costs to fight it exceeding $10 billion a year."

5. Manage IM on your company's network- it's an increasingly important part of IT governance.

Instant messaging (IM), which started out as almost a toy compared to e-mail and the Web (the Internet's killer apps), has grown into a major form of network communication, both within and without corporate networks. The concept wasn't new (the Unix "talk" command had been around for years), but the proprietary and insecure nature of IM made it an immediate security headache.

ServerWatch describes IM as an application that "entered the corporate infrastructure by the back door," and IM security concerns are legitimate.

"For an IM system to work, a user's workstation must broadcast that it is on the network," *ServerWatch* writes. "Once two workstations connect, the conversation takes place across a virtual connection. Most IM systems currently do not support such security staples as authentication and encryption. This means that a hacker can intercept any exchange of information. An unauthorized person also can use an IM connection to access the corporate network and possibly introduce viruses. Further, IM exchanges typically are not logged, and this makes it impossible for corporate management to monitor and control the links."[12]

IM is also a compliance problem. Research firm IDC writes that "Instant Messaging is becoming more similar to e-mail in terms of corporate requirements for tracking and archiving of messages."[13]

Therein lies the problem, for new guidance from the SEC and the National Association of Securities Dealers (NASD) makes clear that relevant IM traffic must be archived and readily produced, just like e-mail and paper documents. "Lack of formality of instant messaging does not exempt it from the general standards applicable to all forms of communication with the public," NASD recently warned.[14]

All of the liability potential that accrues from e-mail also exists in instant messaging. Your company has to decide how to deal with IM. You can decide to block IM traffic entirely, allow the use of only specific IM clients, or restrict the use of IM to certain employees or departments. Since there is no standard protocol for IM send and response, you must be able to recognize traffic from each IM client independently. Ideally, you should be able to filter IM traffic and archive any required by law.

6. Extend your acceptable use policy to cover company's mobile workforce.

Most content control assumes a closed company network — a situation rarely found on the ground. In addition to traditionally mobile elements of the workforce, such as sales departments, companies must now deal with telecommuting, outsourcing and a bewildering array of new methods for employees to connect to the network.

These include traditional dial-up, landline broadband (with and without Virtual Private Network tunneling), paging, 802.11b and 802.11g wireless links and even satellite Internet access.

[12] "Instant Messaging Overview," *ServerWatch*, 11/15/2001.

[13] "Spam and Instant Messaging Usage Are a Rising Threat to E-mail," IDC, 10/30/2003, http://www.idc.com/getdoc.jhtml?containerId=pr2003_10_28_090005

[14] "Clarification for Members Regarding Supervisory Obligations and Recordkeeping Requirements for Instant Messaging," NASD notice to members, July 2003, p. 342.

All of these connections cause problems for traditional intrusion detection and prevention (outside workers must have trusted connections) and for the new world of content control. For companies of any size, the days of Internet traffic feeding through one router to a landline are over.

Tech-research firm Gartner predicts the number of enterprise users with mobile e-mail will grow to at least 10 percent in 2007, up from 1 percent in 2002. Another recent study shows more than 50 percent of laptop users access a wireless network for at least an hour a day.[15]

A content-filtering system must be able to monitor all these points of access; compliance-problematical content can enter through them as easily as it can be generated inside the network.

7. Stop unwanted content to ensure your network is available for business related use.

If you run a decent-sized enterprise network, you probably spend a fair amount of time and money guarding against denial-of-service attacks, outside attacks that flood your Internet connection with packets to prevent access to your Web site or mailserver. Recent distributed denial-of-service attacks have taken down sites at Microsoft and SCO, and their threat is real.

For every network crippled by a DDoS attack, however, thousands are slowed or crippled from within — by unwanted network traffic initiated by employees. Examples are legion — downloading that latest multimegabyte Microsoft service pack, downloading music from peer-to-peer networks such as KaZaA, Grokster, or Aimster (or even new legal services such as Apple's) — all soak up company bandwidth and disk space, making those resources unavailable for legitimate business use.

Other companies have experienced network slowdowns, only to discover a server devoted to Unreal Tournament or other multiplayer games.

Other unwanted traffic comes from outside – Spam being the number-one offender. IDC says spam made up 32% of all external and internal e-mail on an average day in North America in 2003, up from 24% in 2002. "The rising torrents of spam are reducing e-mail's usefulness by forcing users and IT staff to expend additional time and energy to identify, delete, and prevent spam from clogging inboxes," IDC reported.[16]

[15] Power Strategies, August 2003.

[16] "Spam and Instant Messaging Usage Are a Rising Threat to E-mail," IDC, 10/30/2003.

Good network management keeps mailservers as free of spam as possible, hard drives as free of non-business files as possible, and bandwidth as free of non-business traffic as possible. SurfControl can help with all three goals.

SurfControl can recognize and block P2P network traffic, do the same for downloading of particular types of files (media files such as digital video, photographs or audio files, say).

SurfControl's E-mail Filter provides numerous layers of Spam protection, including lexical content scanning, combined with dictionary threshold weighting to avoid false negatives; the Virtual Learning Agent, a neural-network engine that is pre-trained to recognize adult content, and can train itself by scanning previous spam to recognize future spam.

In summary, corporate-governance IT projects are designed to comply with government mandates to retain corporate-governance records and prevent the release of confidential ones. The benefits of such projects, properly applied and managed, however, will leave a legacy of good business practices that will pay off and should be in place, regulations or no.

For more information about SurfControl content filtering solutions, or to download a free trial of SurfControl Web, E-mail or Instant Message Filter, visit www.surfcontrol.com

SurfControl®