Data Loss Protection

# Data Loss Prevention: Keep Sensitive Data-In-Motion Safe

White Paper

WatchGuard® Technologies, Inc.
Published: November 2010

## No Company Is Immune to Data Loss

In today's business environment, media headlines are increasingly featuring data breaches of large magnitudes that put people's personal information at risk, and no country or industry is immune. (Figure 1. Incidents by Business Type - All Time. Source: DATAlossdb.org/statistics). With the changing landscape of business communications and the explosive use of email and Web 2.0 applications for collaboration and business processes, gone are the days when hacking and virus threats were the highest security priority for an organization's IT department. It used to be that organizations were mainly concerned about protecting their data from the outside, but today they also have to protect data from the inside. Sensitive information enters and exits company networks every day. With the evolution of web-based applications, organizations are still largely uncontrolled and unmonitored when it comes to employees using email, social networks, webmail, file transfers, and more.

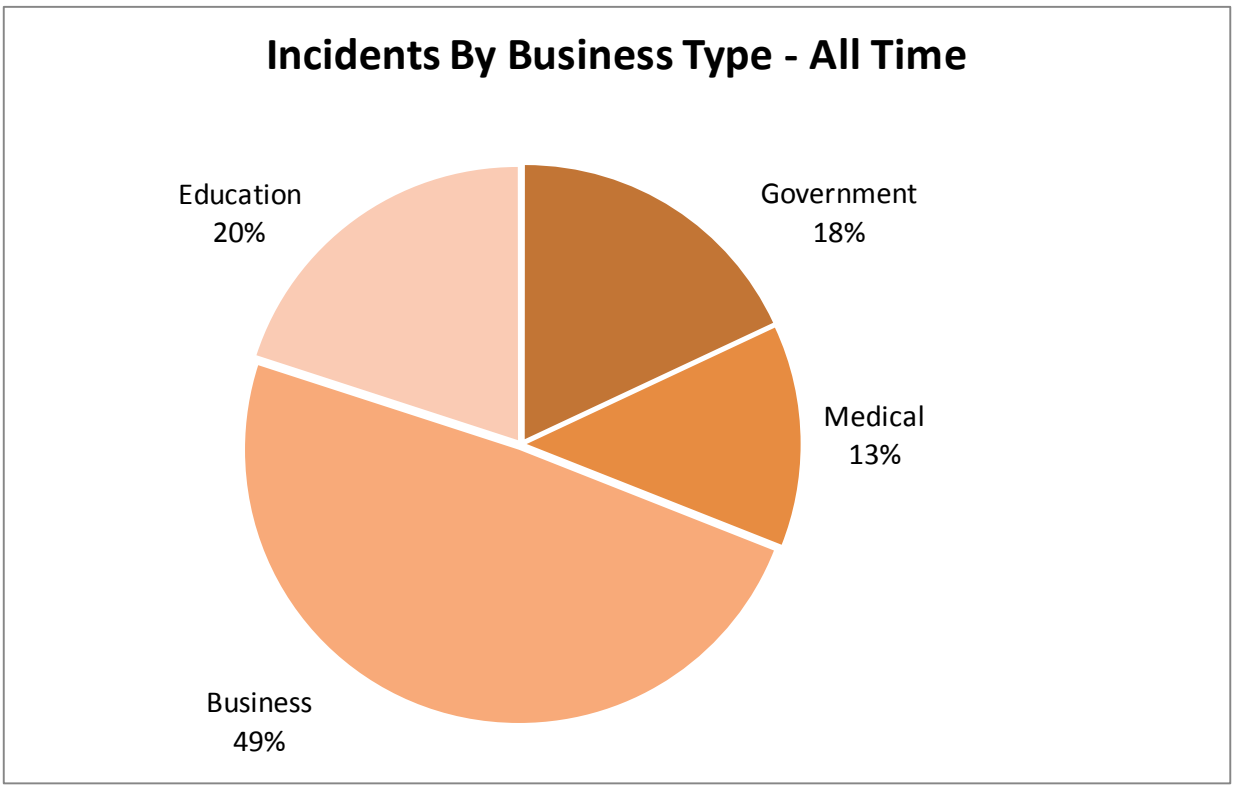


**Figure 1. Incidents by Business Type - All Time (Source: DATAlossdb.org/statistics)**

Organizations now need to be on constant guard against data being lost or stolen. According to KPMG's "Data Loss Barometer," in 2009 alone, more than 113.6 million people were affected by data loss. (See Figure 2. People Affected by Data Loss in 2009.) To put this into perspective, there are approximately 310.5 million people in the United States and 6.9 billion globally.

## Data-in-Motion: A Security Threat to Every Organization

Any time data is set into motion – accessed in an unconventional way, forwarded to a co-worker, sent to a printer, etc. – its security is put at risk. Managing (and controlling) data-in-motion is a requirement for

businesses to function effectively and efficiently. At the same time, it is also a growing security threat. Data loss (or leakage) occurs in every organization either unintentionally or maliciously. In fact, 3 out of 5 organizations have experienced a data loss or theft event,[1] and approximately 9 out of 10 data loss or theft events go unreported.[2]

According to IDC, data-in-motion accounts for more than 83% of all data loss violations and DataLossDB states that 73% of data loss violations are accidental. In addition, all types of data are vulnerable. Why? More and more employees rely on email for business communications and they use email as a central filing system where they store the bulk of their critical business information. This dramatically increases the probability of leaking sensitive or confidential data. All it takes is for a recipient's email address to be misspelled or an incorrect key to be pressed by an employee and a message containing confidential information ends up in the wrong hands. All of us can relate.

At some point or another, we have pressed the send button a little too hastily and realized, after the fact, that our email ended up in an unintended recipient's inbox. In addition, advances in technology make it even easier for this inadvertent data loss to occur. For example, Microsoft Outlook Autocomplete Email Address feature adds a great convenience to our email experience, but if you start typing "susan@bigtaxfirm.com" and the system automatically picks up the first "susan" as being "susan@analystfirm.com" without you noticing that data can end up in the wrong hands and could have a detrimental effect on your business.

**Cause of data loss:**
**People affected in 2009 (January to June)**

| Incident Type | No. of people affected |
|---|---|
| Computer theft/loss | 2,091,422 |
| Hacking | 105,505,536 |
| Hard copy theft/loss | 11,960 |
| Human/system error | 291,417 |
| Improper disposal | 102,035 |
| Malicious insider | 1,555,148 |
| Malware | 34,567 |
| Portable media theft/loss | 1,340,995 |
| Unknown | 49,413 |
| Web/network exposure | 2,700,300 |

Source: KPMG International, September 2009

**Figure 2. People Affected by Data Loss in 2009**

[1] Ponemon Institute: http://www.ponemon.org/news-2/7
[2] Ponemon Institute: Dell + Ponemon Survey

Data loss can be attributed to many factors as outlined in Figure 2 and many of these reasons for data loss can be avoided. To avoid data loss, an organization needs to have a comprehensive data loss prevention solution in place that not only protects networks from inbound threats to data (such as malware, etc.), but also outbound data loss prevention measures need to be addressed to prevent confidential consumer, personal, and sensitive corporate information from exiting the organization.

## The Cost of a Data Breach

Data loss becomes a significant problem and risk as organizations are trying to meet and manage regulatory and internal compliance and control requirements, including:

- **Government & Industry Compliance Regulations:** e.g. HIPAA, PCI, GLBA, SOX, etc.
- **Internal Policies:** C-level rules, sensitive and confidential information
- **Acceptable Use:** HR policies, sexual harassment and legal violations that can occur in messaging
- **Intellectual Property:** Trade secrets, sales reports, financial statements, sales or business plans, etc.

Getting caught losing sensitive data is expensive, disruptive, and damaging to carefully nurtured corporate images. There are significant hard costs to non-compliance in mitigation and remediation to affected individuals such as auditors and board members not to mention regulatory fines and fees to support increased audits. However, often unappreciated are the soft costs to brand equity and competitive advantage which result in lost customers. Enterprises are penalized in both the court of law and the court of public opinion.

If sensitive information is exposed, it's not only the millions of dollars to fix that breach that costs the company, it can wreak havoc on the company in other ways, such as:

- Negative PR
- Brand erosion
- Loss of consumer confidence
- Loss of business partner confidence
- Regulatory fines
- Stock market loss
- Legal fees
- Implementation of internal processes

According to the Ponemon Institute (2009), the total cost of coping with the consequences of a data breach rose to $6.6 million per breach. The day when the fall-out from one data loss incident is sufficient to bankrupt a business may not be far away.

Whether your data loss is accidental or malicious, you need to gain insight into the magnitude of your data loss problem, identify security gaps, and develop a proactive approach to stop data loss before it happens. The vast amount of potential avenues along with the wide array of privacy and security requirements has escalated data loss prevention to become a critical issue that can only be addressed by comprehensive data loss prevention tools that are used to accelerate business, protect your organization, and ensure privacy. Organizations can no longer afford to ignore data security.

## Employees: The Largest Threat Vector to Your Company's Most Critical Assets

While your employees are the most valuable asset to your business they are also the largest threat vector to your most critical business assets. According to a study conducted by the Verizon Business RISK team in cooperation with the United States Secret Service[3], 48% of data breaches are caused by insiders, and 46% of breaches are the result of insider privilege misuse (Figure 3. Types of Misuse by Percent of Breaches[3]).

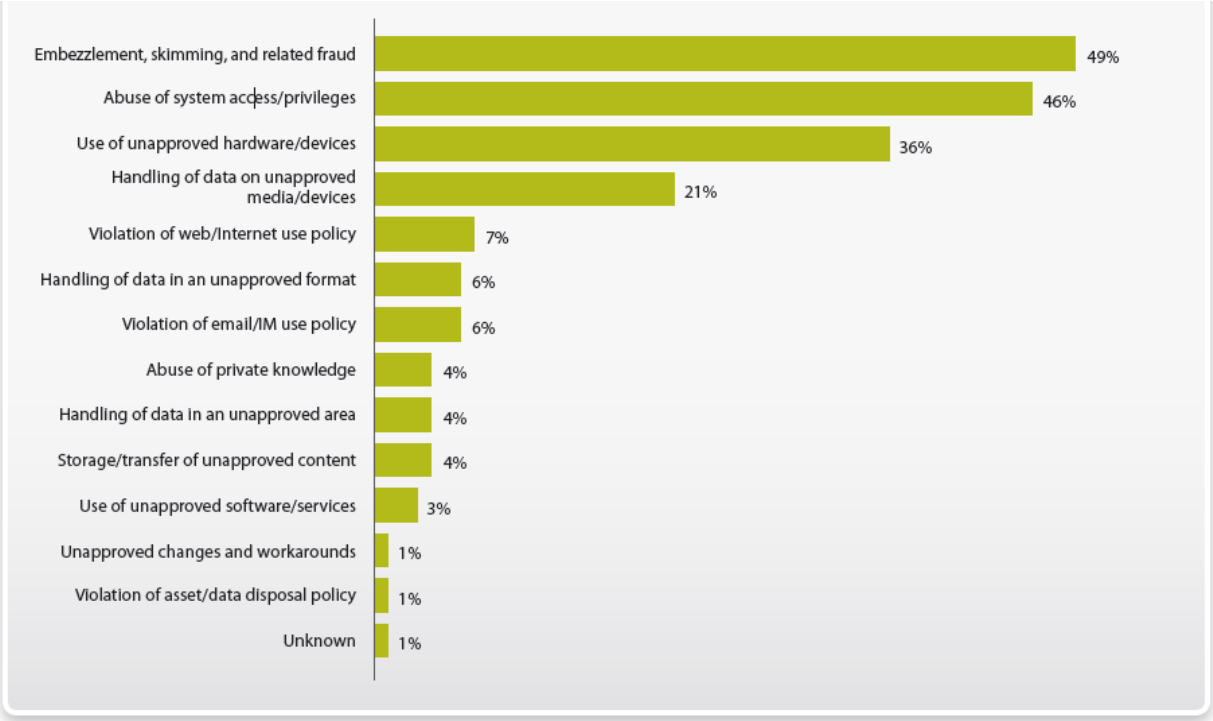


**Figure 3. Types of Misuse by Percent of Breaches[3]**

To put things into perspective, regardless if malicious or accidental, people consistently send, post and discuss corporate intellectual property, confidential information, and sensitive topics with other employees, friends, competitors, partners, etc. over messaging networks. With the proliferation of business communications and transactions conducted via common channels such as email or web, it is inevitable that sensitive or confidential information is being transmitted by employees at every level of the organization. These business communications and enablement tools create a risk boundary through which unauthorized data can escape. When considering how the landscape of business communications, business enablement and web application tools has vastly grown, companies have responded by implementing security policies, procedures, and tools to limit threats to their business critical information and their data-in-motion. Regardless of measures taken, employees around the world still engage in risky behaviors that put corporate and personal data at risk. Without adopting a

[3] Verizon: 2010 Data Breach Investigations Report (http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf )

comprehensive data-in-motion security strategy, sensitive data may be leaving your organization — authorized or unauthorized — and the perpetrators likely reside within your own company walls.

## The Insider Threat Profile

Insider threats to organizational assets — whether it is customer data, intellectual property, payment info, etc. — can be broken down into two types:

1. **The insider who acts with malicious intent:** This is typically someone with administrator rights or privileges to access sensitive information or data such as a sales operations administrator, executive, or employee within the finance department. In each case, this is a trusted employee with normal access rights to confidential data, such as customer credit card or social security numbers, sensitive files, or revenue data. What happens if this employee decides to leave and joins a competitor, or simply tries to trade this information for cash?
2. **The non-malicious insider who violates policy or leak data without necessarily seeking to do so:** For every malicious insider, there are dozens to hundreds of employees who are simply trying to get their work done. In the process, they perform all sorts of unwitting policy violations that put your company's confidential data at risk.

## Risky Employee Behavior and Data Loss

It is rational that not all data loss from within an organization is malicious. In most cases, data loss is the result of common mistakes that employees make. To understand the risks to our confidential data by employees, it is important to understand common risky behavior, as well as common errors that employees make that heighten the risk of data loss.

### Sending Confidential Documents to Personal Email Addresses

Many of us are guilty of this. Rather than take home our company-issued laptops to work on a document that contains sensitive data, we send the document to our personal email account (e.g. Hotmail or Gmail), intending to work on it when we have a moment over the weekend. The issue here is that this behavior poses a high risk to the confidential data being transmitted because these types of applications do not use the same security standards that have been implemented throughout the company email networks. Although you may have stringent policies on what can be sent via email, if you do not have the same protection in place across web, then this sensitive information may be at risk as it passes through mostly unmonitored waypoints.

### Human Error

With all of the automation and new features being introduced in business communications tools and applications today, the likeliness of human error as a threat vector has never been higher. For example, if you consider the Microsoft Outlook AutoComplete Email Address feature whereby the system populates the "To" field in an email by detecting the first few letters input by the sender and populating it with the first name that matches, unless the employee is diligent to ensure that the recipient address is a match, sensitive data can end up in the wrong hands.

### Unauthorized Sharing of Corporate Computer Resources

Many employees bring their company-issued laptops home and share the devices with friends and family members. Occasionally, an employee, in an effort to provide guidance or mentoring to a friend, may even share a document with a personal contact to provide a sample template. Or, on the flip side, an employee may share a confidential document with a friend to get some brainstorming ideas. Consider a third scenario whereby employees do not lock their desktops when leaving their desks, leaving sensitive information exposed should someone access the employee's computer. Although not malicious in nature, this type of behavior is another example of common root causes of unintentional data loss.

### Abuse of System Access and Privileges

System access can be used for any number of malicious tactics by employees, but it also accounts for 46% of data breaches. This involves the malicious use of information assets to which an employee is granted access. Even more alarming is that 51% of data breaches that originate from internal sources are originated from regular employees – Figure 4 below.

| | |
|---|---|
| Regular employee/end user | 51% |
| Finance/accounting staff | 12% |
| System/network administrator | 12% |
| Executive/upper management | 7% |
| Helpdesk staff | 4% |
| Software developer | 3% |
| Auditor | 1% |
| Unknown | 9% |

**Figure 4: Sources of Internal Data Breaches**[4]

These are just some examples of risky employee behavior that contribute to the likelihood of unauthorized data loss. Now, more than ever, companies have to be diligent at not only creating a strong data loss prevention policy management program, but implementing and monitoring it to identify violations and security gaps. Organizations owe it to themselves and their customers to keep information from falling into the wrong hands. At the same time they need to ensure that legitimate business processes and communications are not hindered.

An effective data loss prevention (DLP) solution can accomplish this by providing the ability for compliance and policy officers to create granular outbound policies by user, group or domain. Different people have varying roles and responsibilities; having a DLP solution that recognizes this and enforces

[4] Verizon: 2010 Data Breach Investigations Report (http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf)

appropriate, user- or group-level policies while not hindering the regular course of business is imperative.

## Data Loss Prevention Defined

**Data Loss Prevention** is a security term that refers to a solution that identifies, monitors, and protects sensitive data to detect and prevent the unauthorized use and transmission of confidential information.

Data Loss Prevention is:

- A business tool that requires a comprehensive strategy
- Technology that inspects sensitive content, and audits and enforces content use policies

Data Loss Prevention can be used for:

- Regulatory due diligence
- Intellectual property protection
- Accidental data loss
- Data theft

DLP is a highly discussed, and debated, technology that is designed to monitor and filter content. Like any new technology and approach that addresses business processes, compliance and privacy, DLP can be viewed either as a tool or as a standalone product. Based on recent events, customer deployments and analyst research, DLP has migrated from a standalone product that affected the entire enterprise, computing systems and business processes to one of a tool that is used to accelerate business, protect the organization and ensure privacy. Evidence of this can be easily seen with acquisitions in the space that are incorporating DLP into existing solutions as a complement – not as a silo.

An effective data loss prevention solution needs to be:

- Seamlessly integrated with a secure content and threat management platform
- Able to scan across email and web with consolidated policies, management and administration
- Automated with no additional FTEs required
- Have a low cost of entry with low total cost of ownership

DLP products are intended to help prevent (and detect) the unauthorized disclosure of data, whether that data is sensitive, regulated, or even classified.

## The Solution: WatchGuard XCS Data Loss Prevention

The WatchGuard XCS solution is a best-of-breed, easy-to-use, all-in-one suite of products for defense-in-depth for email security, web security and data loss prevention. It uses a seamlessly integrated process for securing content from data loss while controlling confidential information as it moves across network boundaries. This allows organizations to protect data that traverses their network to prevent accidental or malicious data leakage.

XCS Data Loss Protection, built within the WatchGuard XCS platform, is a single-solution business tool that enables organizations to:

*Define Policies either by utilizing pre-defined dictionaries within XCS or from a business's own custom dictionaries*

*Indentify Sensitive or Protected Content with deep content inspection across email and web to prevent accidental and malicious leakage through the vast messaging mediums*

*Enforce Policies of the identified content with WatchGuard XCS's integrated remediation capabilities, including allowing, blocking encrypting, blocking, blind-copying, or quarantining messages*

WatchGuard XCS DLP is unique as it provides a deep content inspection and contextual analysis approach to determine the sensitivity or confidential nature of a message and its content and assesses the appropriate remediation that needs to be applied. This is done by:

- **Content Analysis** - Determining what is being delivered (content inspection), including files and attachments, and comparing it to policies in an effort to discover policy violations.
- **Contextual Analysis** - XCS DLP functionality goes one step further and inspects the context of the traffic. It applies intelligence to determine, based on policies, whether the discovered/identified confidential content that has passed through the content inspection engine is allowable. The system inspects who is sending the content and where or whom the content is being sent to, which is vital in determining if the content is a violation or note, and which proper remediation tactic to employ.

Without context analysis, a typical data loss prevention system would easily block or quarantine important communication with the potential to impede business processes and productivity. Adding to this, DLP can be extended to web traffic using the two above methods.

**XCS DLP WIZARD**

XCS solutions include a DLP Wizard that gives administrators the ability to create data loss prevention policies quickly and simply.

- Users are guided through the configuration of the DLP content control and rules for inbound and outbound email and web traffic
- Users can select specific DLP and compliance tasks such as blocking credit card or national identification numbers, or use a compliance dictionary to scan for specific words or phrases in email and web traffic.
- Remediation actions are provided for each DLP task from a simple drop-down menu. All of this can be done in a few simple steps.

Once users have completed the DLP Wizard, the system will automatically configure the policies on the XCS appliance without any further action required.

## XCS Integrated Data Loss Prevention Process = No Manual Intervention for Always-On Data Loss Prevention

The implementation of DLP provides comprehensive, instant protection from information loss. It uses an integrated process for inspection, discovery, and remediation of policy violations for outbound communications containing sensitive content. Figure 5. Integrated Process for Privacy and Compliance Protection, illustrates this integrated process.

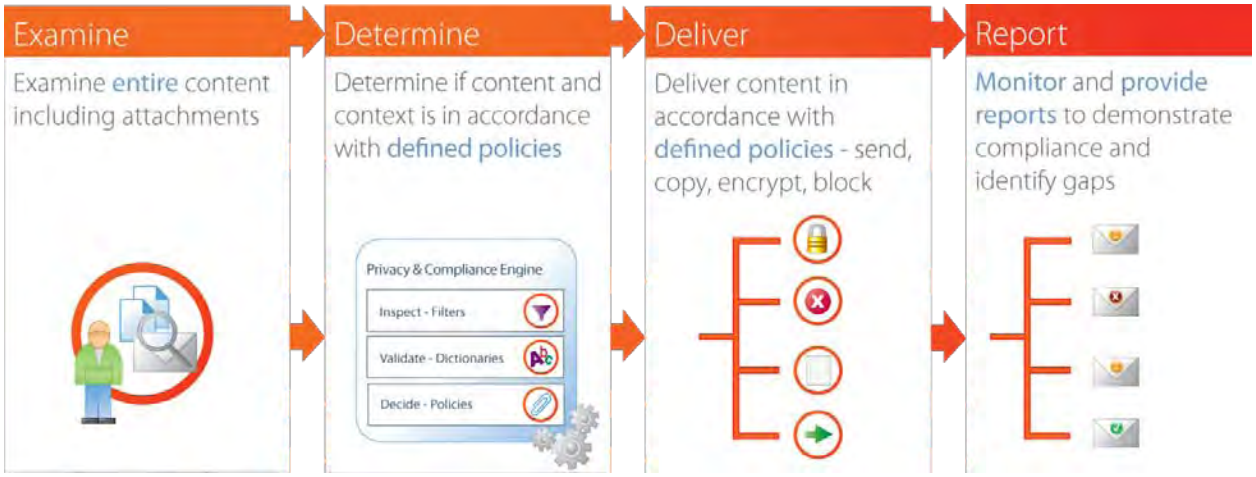


**Figure 5. Integrated Process for Privacy and Compliance Protection**

## Eliminate Data Loss Gaps: Extend Data Loss Prevention to Web Traffic

The Internet provides many exit points for sensitive information to leave your organization. Communications sent by Internet mail, wikis, blogs, and social networks are now a major threat. Adding a web security solution that extends the data loss prevention capabilities provides consolidated visibility and control so you can meet stringent compliance requirements.

When investigating the various methods for data-in-motion protection of data leakage, it is vital to evaluate the entire landscape of content that employees use today. Today's employee has instant access to the web and email through which content can escape, including sending data via popmail systems such as Hotmail®, wikis, blogs, and sending messages and files via email to unlimited, unknown and mostly unrestricted recipients. This fact highlights the risks of DLP as a silo, versus a consolidated platform. The security and administration risks are gaps that place policies into various places in the network versus a single location. Further broadening the gap are disparate scanning of email and web mediums, and reporting DLP activities and violations across multiple protocols and technical silos.

With the WatchGuard XCS appliances, DLP is provided for both email and web protocols in a single administrative access point for creating, managing and enforcing policies for protecting your organization from leakage. WatchGuard XCS DLP is not only transparent from end-users as a gateway appliance, it provides effective and efficient security. Adding a WatchGuard XCS Web Security subscription to your XCS appliance allows you to extend your data loss protection to monitor beyond just SMTP traffic for comprehensive protection across email and web protocols. This comprehensive visibility and protection is now a necessity rather than an option. With the XCS Web Security

subscription, you can scan content in all outbound web traffic, including attachments, for policy violations; it inspects context in sent communications including who is sending the data, where it is being sent, and to whom. To make this easy, it uses the same policies developed for your organization's email communications to save time and ensure strong and consistent enforcement. Administrators can easily manage data loss prevention across protocols from one easy-to-use administrative console.

Overall, a DLP solution must be able to effectively and comprehensively detect attempted policy violations. This includes:

- Multi-protocol monitoring and prevention
- Content-level analysis of all major file and attachment types
- Selective blocking and/or quarantining of messages
- Automatic enforcement of corporate encryption policies

For compliance with regulations such as HIPAA and PCI, protection of intellectual property, and enforcement of appropriate use policies, a DLP solution for data-in-motion will help address one of the most significant vectors for data loss: electronic communications.

Find out more about WatchGuard Data Loss Protection and the XCS family of network security appliances at www.watchguard.com, or contact your local reseller, or call WatchGuard directly at 1.800.734.9905 (U.S. Sales) or +1.206.613.0895 (International Sales).

**ADDRESS:**
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

**WEB:**
www.watchguard.com

**U.S. SALES:**
+1.800.734.9905

**INTERNATIONAL SALES:**
+1.206.613.0895

**ABOUT WATCHGUARD**

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.