



## IronPort Gateway Security Products

*Secure Your Email &  
Make Compliance Easy*



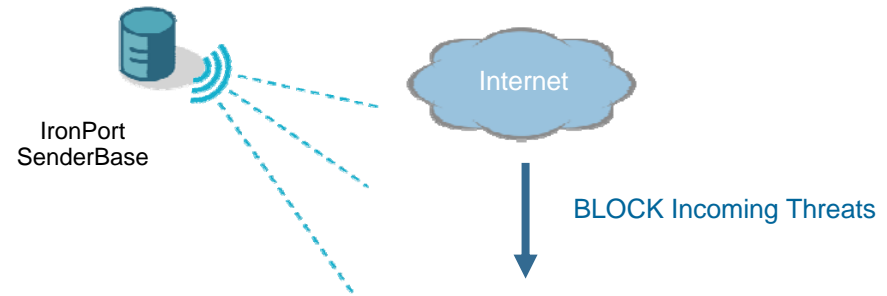
**Anurak Chuetanapinyo**  
***Technical Consultant – Thailand and Vietnam***  
**IronPort Systems, A Cisco Business Unit**

[anurak@ironport.com](mailto:anurak@ironport.com) / [anurak@cisco.com](mailto:anurak@cisco.com)

IronPort is now  
part of Cisco.



# IronPort® Gateway Security Products



## APPLICATION-SPECIFIC SECURITY GATEWAYS



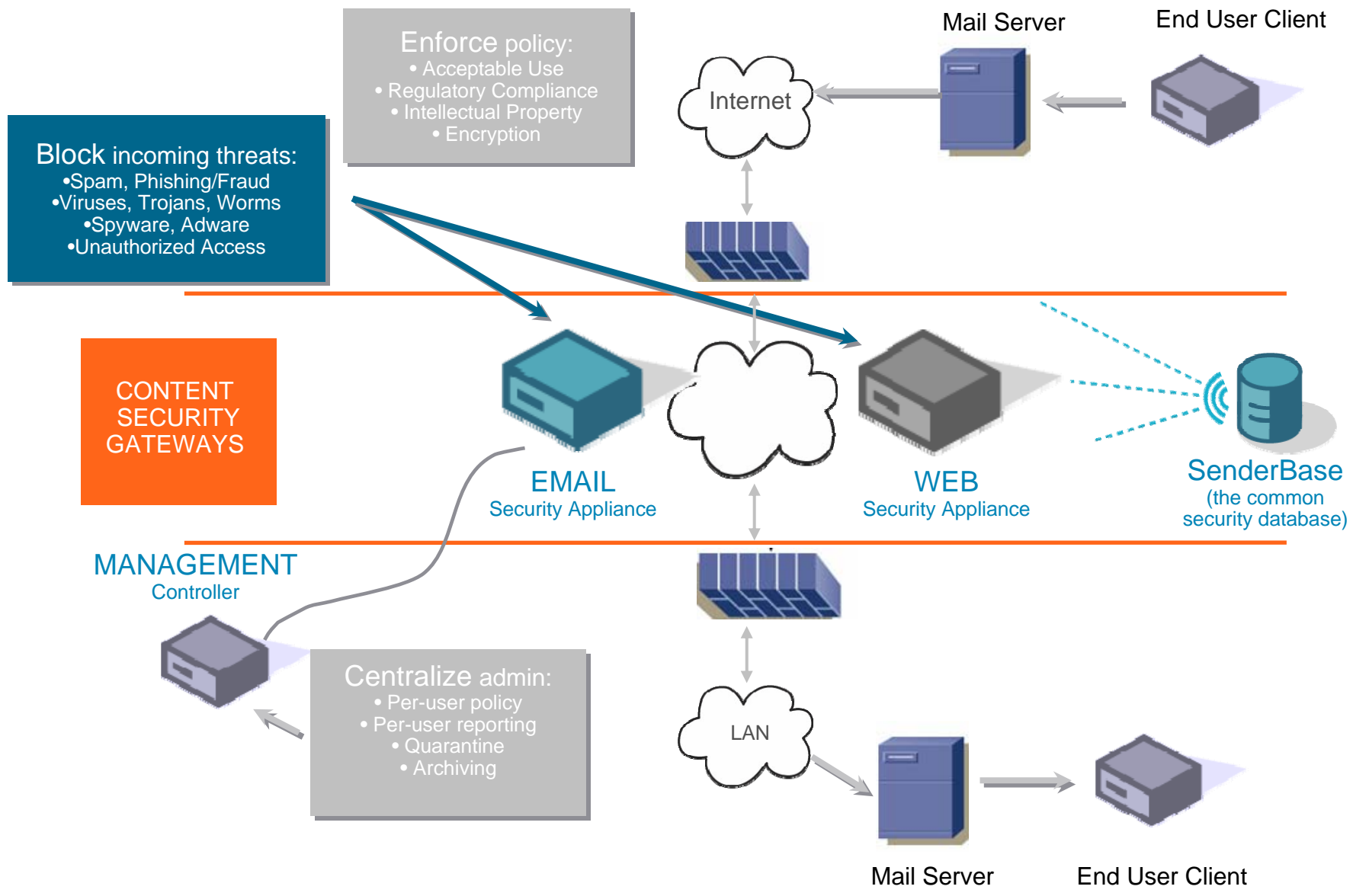
## CENTRALIZE Administration



PROTECT Corporate Assets  
Data Leakage Prevention  
Encryption



# Control at the Edge



# หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทาง คอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐



พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

- “ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึง **แหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ** ที่เกี่ยวข้องกับ การติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

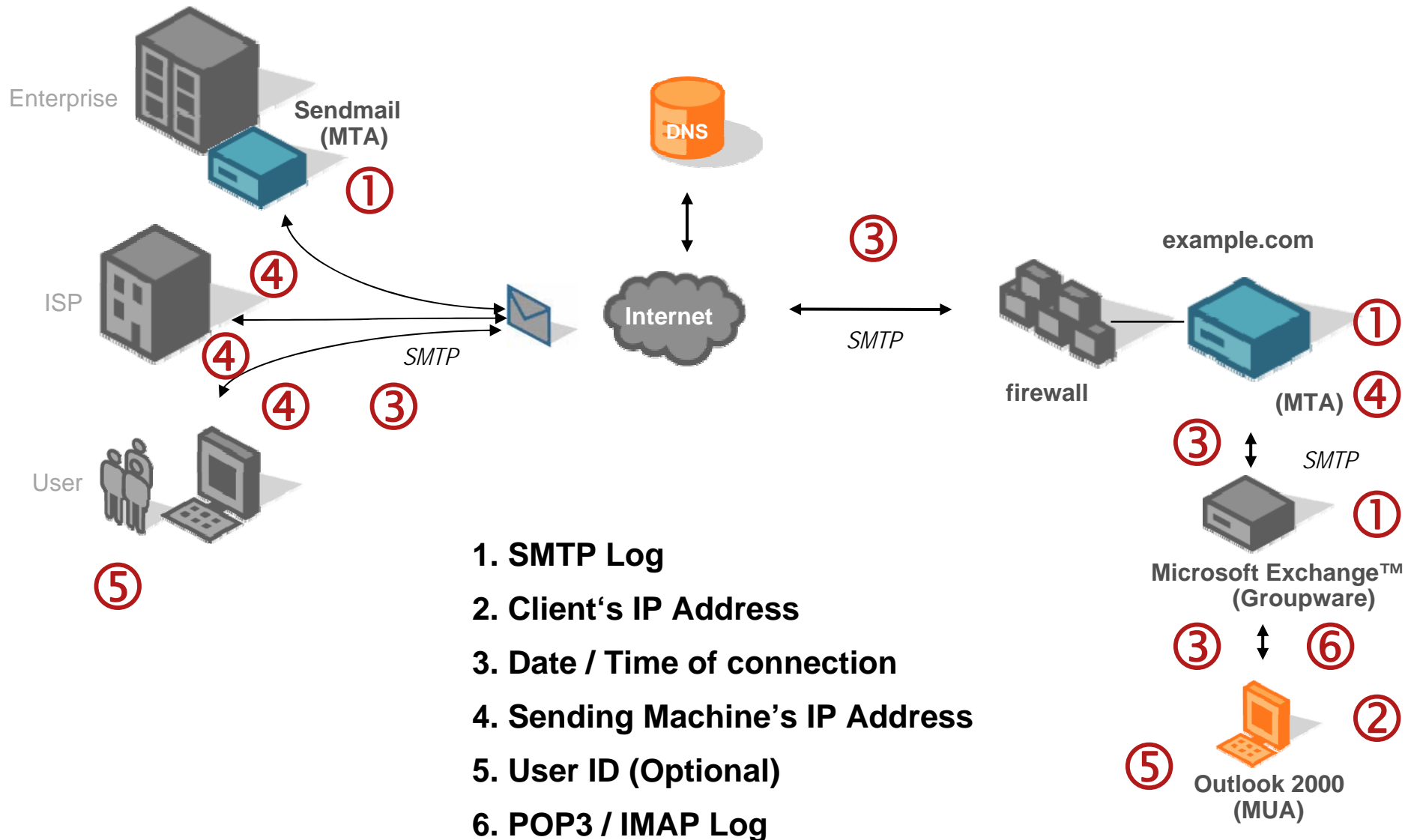
# ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการ จดหมายอิเล็กทรอนิกส์

1. ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ (SMTP Log)
  - หมายเลขของข้อความที่ระบุใน Email (Message ID)
  - Email address ของผู้ส่ง (Sender Email Address)
  - Email address ของผู้รับ (Receiver Email Address)
  - สถานะในการตรวจสอบ (Status Indicator) เช่น ส่งสำเร็จ, ตีกลับ, หรือส่งล่าช้า เป็นต้น
2. ข้อมูล IP Address ของเครื่องคอมพิวเตอร์ผู้ให้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ (Client IP Address)
3. ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการ (Date/Time of Client's connection)

## ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการ จดหมายอิเล็กทรอนิกส์

4. ข้อมูล IP Address ของเครื่องบริการจดหมายอิเล็กทรอนิกส์ที่ถูกเชื่อมต่ออยู่ในขณะนั้น (Sending Machine's IP Address)
5. ข้อมูลชื่อผู้ใช้งาน (User ID) (ถ้ามี)
6. ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการเข้าถึงเพื่อเรียกข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึงไปนั้นไว้ที่เครื่องให้บริการ (POP3 Log or IMAP4 Log)

# Day in the Life of an Email



# IronPort Text Mail Logs

- Contain details of message receiving, delivery, and bounces
- Use cases
  - Track the receipt, processing, and delivery of specific messages
  - Track anti-spam and anti-virus checking results
  - Analyze system performance
- How event records are identified
  - New        New connection initiated; ICID created
  - ICID       Incoming Connection ID
  - Start      New message started; MID created
  - MID       Message ID
  - RID       Recipient ID
  - DCID      Delivery Connection ID
  - Done      Command Complete
  - Ready     System waiting for next command in SMTP



# IronPort Text Mail Logs

## *Example*

**Mon Jun 16 16:57:21 2008** Info: New SMTP ICID 10 interface data1 (10.10.10.10) address **192.168.10.10** reverse dns host someone.somedomain.net verified yes

Mon Jun 16 16:57:21 2008 Info: ICID 10 RELAY SG None match ALL SBRS not enabled

Mon Jun 16 16:57:22 2008 Info: Start MID 50 ICID 10

Mon Jun 16 16:57:22 2008 Info: MID 50 ICID 10 From: **<sender@somedomain.net>**

Mon Jun 16 16:57:22 2008 Info: MID 50 ICID 10 RID 0 To: **<reciepiant@anotherdomain.com>**

Mon Jun 16 16:57:22 2008 Info: **MID 50 Message-ID '<48563828.000022.04736@SOME-D490A4A453>'**

Mon Jun 16 16:57:22 2008 Info: MID 50 Subject '**An Example**'

Mon Jun 16 16:57:22 2008 Info: MID 50 ready 50 bytes from <sender@somedomain.net>

Mon Jun 16 16:57:22 2008 Info: MID 50 matched all recipients for per-recipient policy DEFAULT in the inbound table

# IronPort Text Mail Logs

## *Example*

Mon Jun 16 16:57:22 2008 Info: ICID 10 close

Mon Jun 16 16:57:23 2008 Info: MID 50 **antispam negative**

Mon Jun 16 16:57:23 2008 Info: MID 50 interim AV verdict using Sophos CLEAN

Mon Jun 16 16:57:23 2008 Info: MID 50 interim AV verdict using McAfee CLEAN

Mon Jun 16 16:57:23 2008 Info: MID 50 **antivirus negative**

Mon Jun 16 16:57:23 2008 Info: MID 50 queued for delivery

Mon Jun 16 16:57:23 2008 Info: New SMTP DCID 5 interface 10.10.10.20 address  
**172.16.0.10** port 25

Mon Jun 16 16:57:23 2008 Info: Delivery start DCID 5 MID 50 to RID [0]

Mon Jun 16 16:57:24 2008 Info: Message done DCID 5 MID 50 to RID [0]

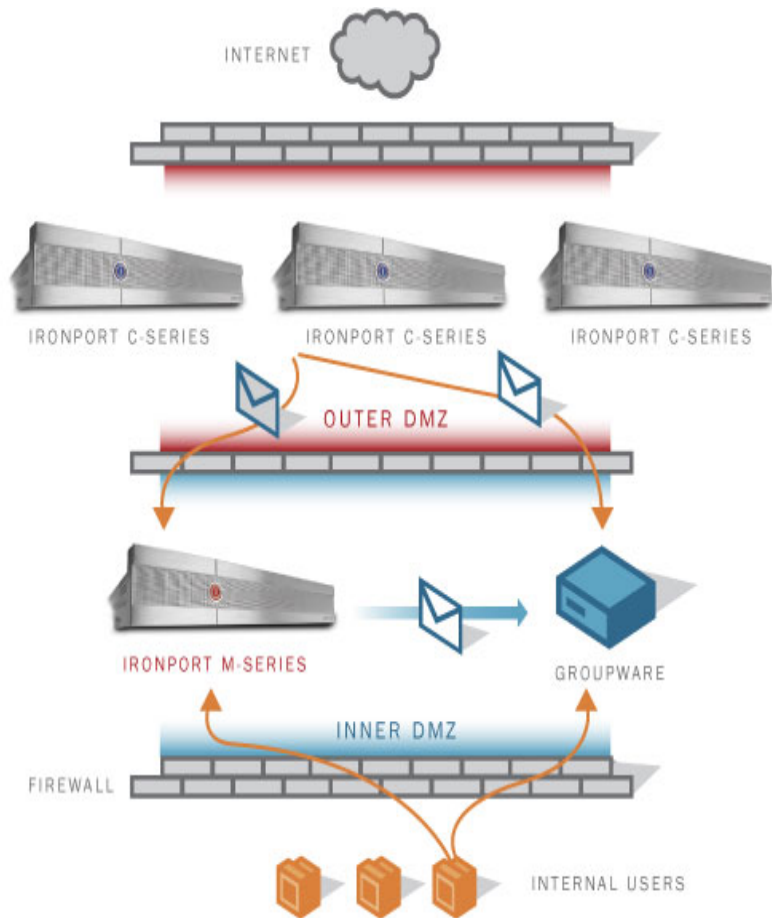
Mon Jun 16 16:57:24 2008 Info: **MID 50 RID [0] Response 'ok: Message 34543  
accepted'**

Mon Jun 16 16:57:24 2008 Info: Message finished MID 50 done

Mon Jun 16 16:57:24 2008 Info: DCID 5 close



# หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐



- 8. การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคง ปลอดภัย
  - 1. เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้
  - 2. มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บและกำหนดลำดับในการเข้าถึงข้อมูลดังกล่าว เพื่อกำหนดไม่ให้ผู้ไม่ได้รับอนุญาตเข้ามาแก้ไขข้อมูล
  - 3. จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ เพื่อให้การส่งมอบ ข้อมูลนั้น เป็นไปด้วยความรวดเร็ว
  - 4. ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ให้บริการเป็นรายบุคคลได้จริง (Identification and Authentication)

# IronPort Message Tracking

*Easiest way to see what happen to your email*

1

**Message Tracking**

No Tracking Data is currently available. Data in time range: 58.6% complete

Envelope Sender: [?] Is [ ]

Envelope Recipient: [?] Is [ ]

Subject: Is [ ]

Date and Time Range: Start Date: [ ] Time: [ ] and End Date: [ ] Time: [ ]

Advanced

Sender IP Address: [ ]

Search rejected connections only  Search messages

Message Event: *Selecting multiple events will expand your search to include messages that match each event type.*

Virus Positive  Hard bounced

Spam Positive  Soft bounced

Suspect Spam  Currently in Outbreak Quarantine

Delivered

Message ID Header: [ ]

IronPort MID: [ ]

IronPort Host: [ Select Host ]

3

**Message Tracking**

Available Data: 05 Jun 2007 14:00 to 06 Jun 2007 14:12 (GMT -0700)

Search

Envelope Sender or Sender IP: [?] Contains [ ] tacoma

Envelope Recipient: [?] Contains [ ] ironport.com

Subject: Begins with [ ]

Date and Time Range: Start Date: [ ] Time: [ ] End Date: [ ] Time: [ ]

Clear Submit

Generated: 05 Jun 2007 14:00 (GMT -0700)

Results Items per page 10

Displaying 1 — 4 of 4 items.

1	Thu Jul 22 2005 16:37 (GMT -0700)	MID: 90009054	HOST: mailman.domain.com	Show Details
SENDER: normal_sender@29801.tacoma				
RECIPIENT: janedoe@ironport.com				
SUBJECT: (no subject)				
LAST STATE: Message successfully delivered				

2	Thu Jul 22 2005 16:37 (GMT -0700)	MID: 988809854	HOST: mailman.domain.com	Show Details
SENDER: normal_sender@29801.tacoma				
RECIPIENT: janedoe@ironport.com				
SUBJECT: (no subject)				
LAST STATE: Message successfully delivered				

3	Thu Jul 22 2005 16:37 (GMT -0700)	MID: 988809854	HOST: mailman.domain.com	Show Details
SENDER: normal_sender@29801.tacoma				
RECIPIENT: janedoe@ironport.com				
SUBJECT: (no subject)				
LAST STATE: Message successfully delivered				

4	Thu Jul 22 2005 16:37 (GMT -0700)	MID: 90009054	HOST: mailman.domain.com	Show Details
SENDER: normal_sender@29801.tacoma				
RECIPIENT: janedoe@ironport.com				
SUBJECT: (no subject)				
LAST STATE: Message successfully delivered				

Displaying 1 — 4 of 4 items.

2

**Message Details**

**Envelope and Header Summary**

Received Time:	05 Jun 2007 14:00 (GMT -0700)
MID:	167660
Message Size:	905 Bytes
Subject:	(no subject)
Sender:	tacozilla@tacomaterritory.com
Recipients:	brightmail@d1.qa41.qa, brightmail@d1.qa41.qa
Message ID Header:	5bt4b585a9f@a020.d2.clayton.qa
Receiving Host:	ironport.qa
Receiving IP:	172.22.141.2
SMTP Auth User ID:	N/A

**Sending Host**

Reverse DNS Hostname:	ironport.qa (verified)
IP Address:	172.22.141.2
SBR5 Score:	N/A

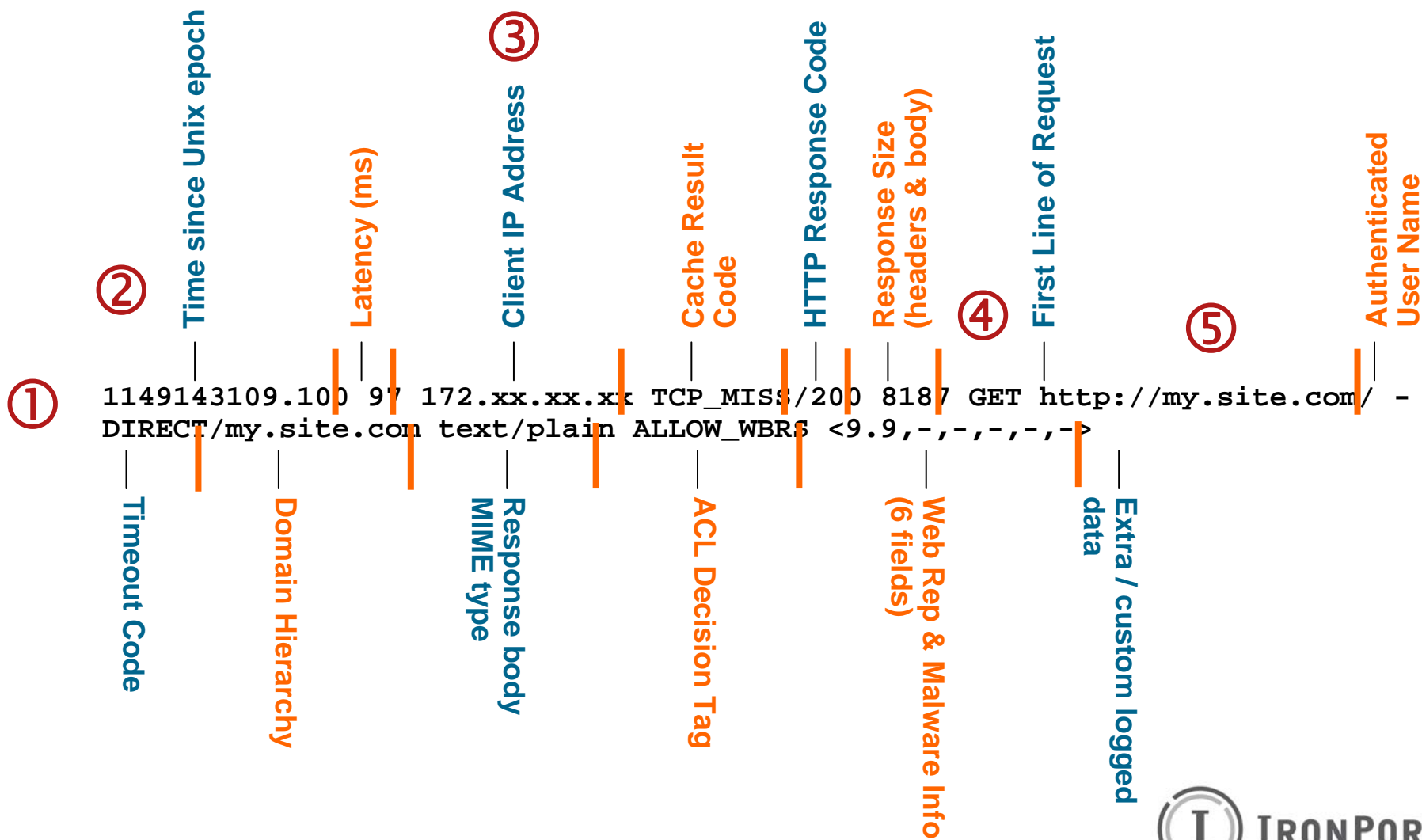
**Processing Details**

Sep 18, 2006 12:11:40 -0800	Message enqueued
Sep 18, 2006 12:11:40 -0800	Message enqueued
Sep 18, 2006 12:11:40 -0800	MAIL POLICY "DEFAULT" PROCESSING brightmail@d1.qa41.qa
Sep 18, 2006 12:11:40 -0800	Message processed by Anti-spam. Verdict: Negative
Sep 18, 2006 12:11:40 -0800	Message processed by Sophos Anti-Virus. Verdict: Negative
Sep 18, 2006 12:11:40 -0800	Message queued for delivery
Sep 18, 2006 12:11:40 -0800	Message successfully delivered to brightmail@d1.qa41.qa at '172.21.141.1'. Response: "sent"
Sep 18, 2006 12:11:40 -0800	MAIL POLICY "DEFAULT" PROCESSING brightmail@d1.qa41.qa
Sep 18, 2006 12:11:40 -0800	Message processed by Anti-spam. Verdict: Negative
Sep 18, 2006 12:11:40 -0800	Message processed by Sophos Anti-Virus. Verdict: Negative
Sep 18, 2006 12:11:40 -0800	Message queued for delivery
Sep 18, 2006 12:11:40 -0800	Message successfully delivered to brightmail@d1.qa41.qa at '172.21.141.1'. Response: "sent"
Sep 18, 2006 12:11:40 -0800	MAIL POLICY "ipas_drop" PROCESSING ipas_drop@d1.qa41.qa
Sep 18, 2006 12:11:40 -0800	Message processed by Anti-Spam. Verdict: Suspected spam
Sep 18, 2006 12:11:40 -0800	MAIL POLICY "ipas_drop" PROCESSING ipas_drop@d1.qa41.qa
Sep 18, 2006 12:11:40 -0800	Message processed by Anti-Spam. Verdict: Suspected spam

## ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ

1. ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการเว็บ
2. ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการ (Date/Time of Client's connection)
3. ข้อมูล IP Address ของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ (Client IP Address)
4. ข้อมูลคำสั่งการใช้งานระบบ
5. ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI: Uniform Resource Identifier)

# IronPort Web Access Logs



# IronPort Systems Data Loss Prevention

*PROTECTING SENSITIVE COMMUNICATIONS*



# Accidental Information Loss is on the rise...

## Confidential Information is at risk...



On TechRepublic: 4

**cnet NEWS.com** Search:

Today on CNET | Reviews | News | Downloads | Tips & Tricks | CNET TV | Compare Prices

Business Tech | Cutting Edge | Green Tech | Access | Security | Media 2.0 | Markets | Per

### Verizon gaffe lets customer details slip

By Joris Evers  
Staff Writer, CNET News.com  
Published: August 23, 2006, 5:11 PM PDT

TalkBack | E-mail | Print | del.icio.us | Digg this

**Verizon Wireless this week accidentally distributed a file with limited details on more than 5,000 customers outside the company, potentially giving identity thieves a toehold.**

The Microsoft Excel spreadsheet file was e-mailed on Monday and includes names, e-mail addresses, cell phone numbers and cell phone models of 5,210 Verizon Wireless customers, going by a copy of the file obtained by CNET News.com. All of the customers have Motorola Razr phones, according to the spreadsheet.

The spreadsheet was inadvertently sent to about 1,800 people, all Verizon Wireless subscribers, according to a follow-up e-mail apologizing for the gaffe that the mobile carrier sent on Thursday. The Excel file was attached to an ad for a Bluetooth wireless headset, instead of the electronic order form that was supposed to be sent.



Sony Ericsson's Q3 Report Leaked - Sales of Camera and Music Phones Soar | Digital Media Wire - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.dmwmedia.com/news/2006/10/11/sony-ericsson-s-q3-report-leaked-sales-of-camera-and-musi

Getting Started Latest Headlines

**dmw digitalmediawire** connecting people & knowledge

home events directory newsletter advertise rss about

music games internet video mobile marketing deals jobs

law investing commerce tech metrics classifieds career moves

The content delivery network for digital media... Find out how to **optimize your streaming content** click now!

Sponsor Spotlight @HIRE

Latest Top Stories

- Citing Youth Internet Addiction, China Bans New 'Net Cafes for 2007
- Internet TV Distributor Narrowstep Raises \$7.1 Million
- Activision to Buy Multiplayer Game Technology Firm DemonWare
- GDC: Telephia Reports Revenue Increase in Mobile Games
- Online Social Network for

Home » content

### Sony Ericsson's Q3 Report Leaked - Sales of Camera and Music Phones Soar

Submitted by Jay Baage on October 11, 2006 - 8:20am

Sony Ericsson surprised the market in two ways on Wednesday. First, their Q3 2006 report leaked out one day in advance. Secondly, the results were much better than the market was expecting. Sales of cell phones with high-resolution digital cameras and Walkman music players have exploded in the third quarter. Net income increased by 187% to \$374 million year-on-year. Shares in Ericsson rose by 5% on the Stockholm Stock Exchange, while Sony was up by 4% on the NYSE Wednesday afternoon.

Upcoming DMW Events

- FUTURE OF FILM**  
March 21, 2007 | LA  
www.lafilmconference.com
- The Millennials**  
April 18, 2007 | LA  
www.millennialsconference.com

Events Calendar  
Sponsorship Opportunities (PDF)  
Submit a Speaker

Around the Web

- Yahoo Slashes Semel's Stock Bonus (Reuters)

# Evolution of Data Loss

## Email Remains A Primary Loss Vector

**Errant e-mails compromise hundreds of student IDs**  
 Student Financial Services sends 632 registration block notifications containing students' Social Security numbers to the wrong students

Breanna Hockenbury, Cavalier Daily Staff Writer

Notifications from Student Financial Services intended for students whose registration was blocked were erroneously sent to the wrong students in emails that included others' Social Security numbers.

Student Financial Services intended to send 1,264 emails to alert students of registration blocks. Only 632 e-mails were actually sent.

**SAIC warns of possible data breach** *AP Associated Press*

By Donna Borak, AP Business Writer | July 20, 2007

WASHINGTON --Pentagon contractor SAIC Inc. may have compromised personal information about more than half a million military personnel and their relatives because it did not encrypt data transmitted online.

**Verizon gaffe lets customer details slip**

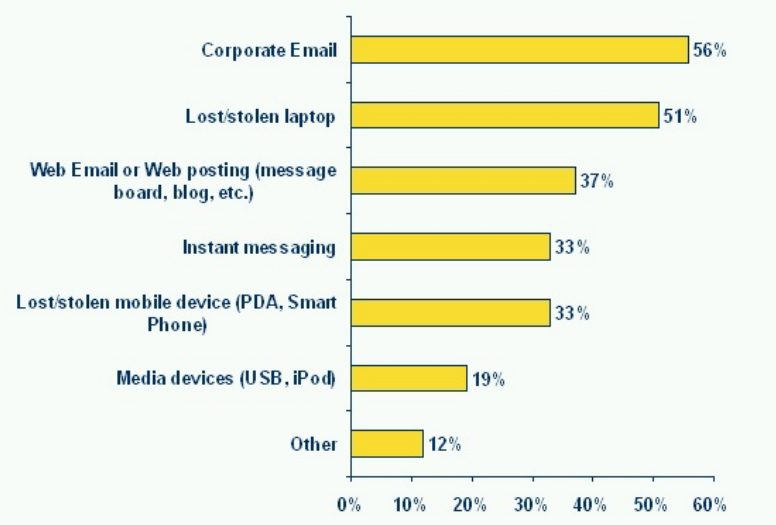
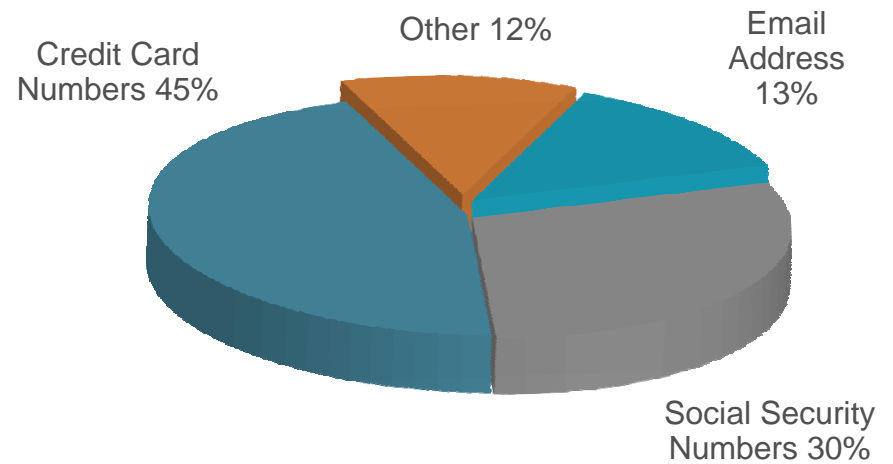
By Joris Evers  
 Staff Writer, CNET News.com  
 Published: August 25, 2006, 5:11 PM PDT

Verizon Wireless this week accidentally distributed a file with limited details on more than 5,000 customers outside the company, potentially giving identity thieves a toehold.

The Microsoft Excel spreadsheet file was e-mailed on Monday and includes names, e-mail addresses, cell phone numbers and cell phone models of 5,210 Verizon Wireless customers, going by a copy of the file obtained by CNET News.com. All of the customers have Motorola Razr phones, according to the spreadsheet.

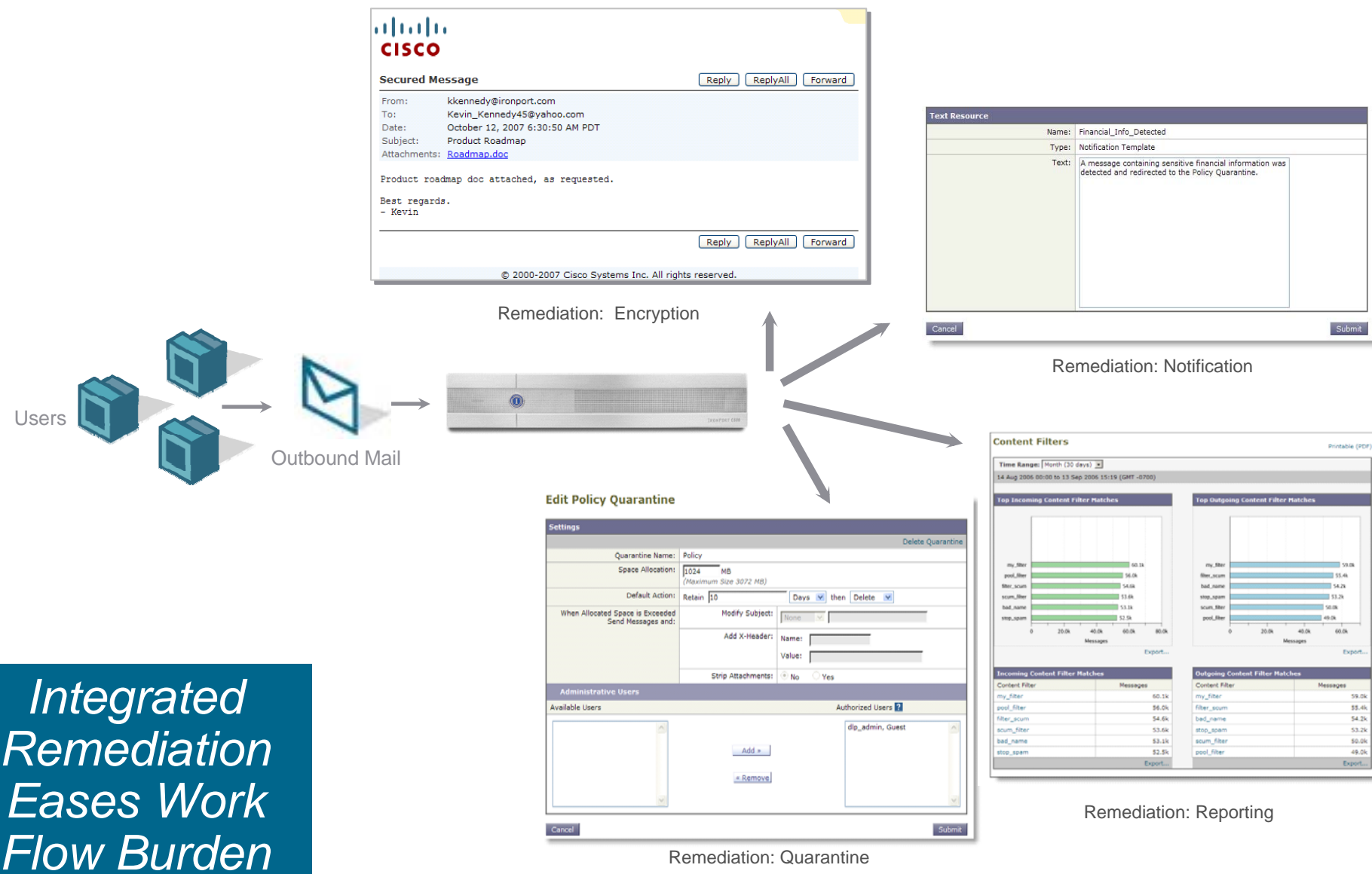
The spreadsheet was inadvertently sent to about 1,800 people, all Verizon Wireless subscribers, according to a follow-up e-mail apologizing for the gaffe that the mobile carrier sent on Thursday. The Excel file was attached to an ad for a Bluetooth wireless headset, instead of the factory order form that was supposed to be sent.

### Record Type Lost



# Data Loss Prevention Foundation

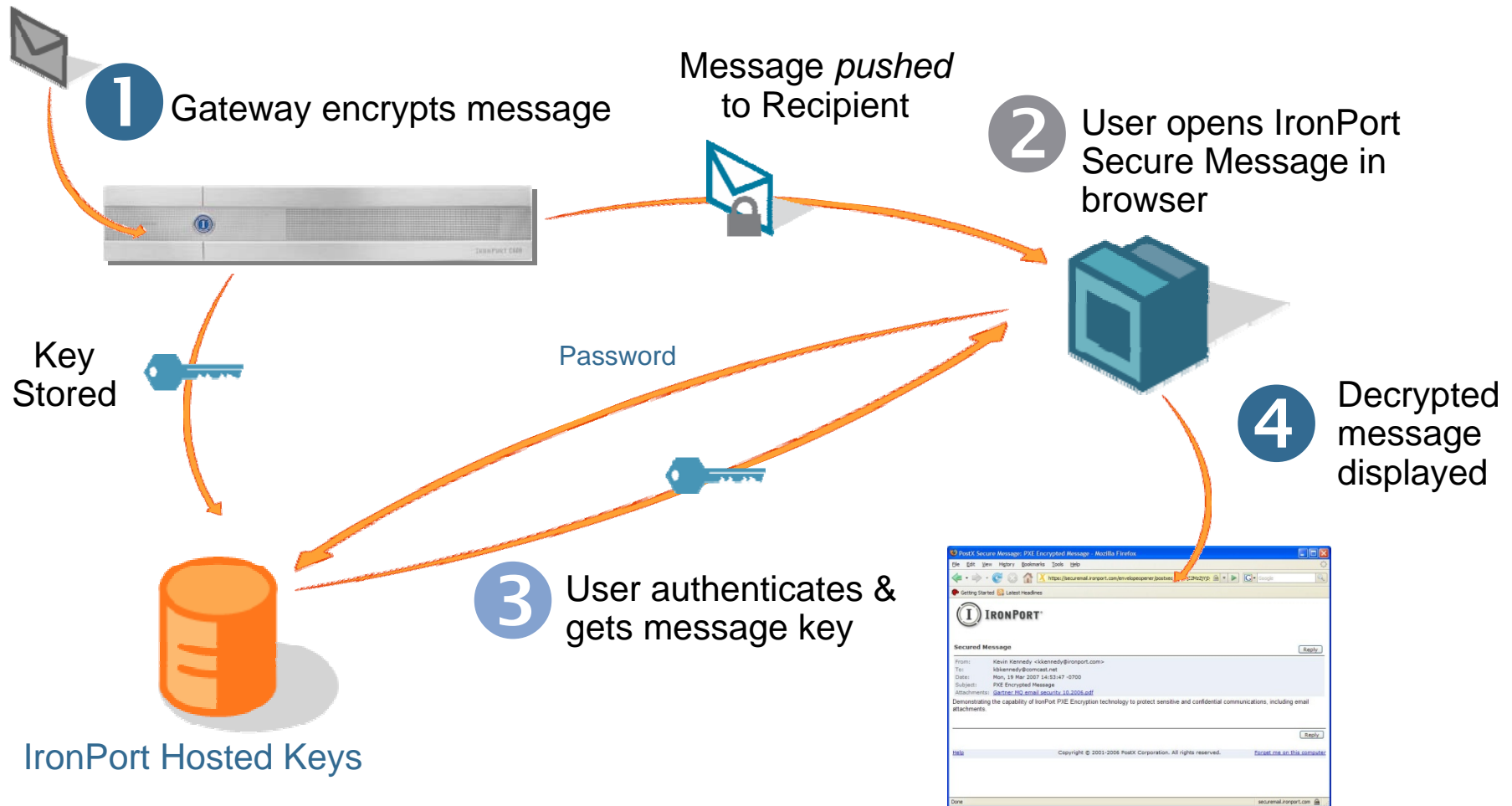
## Integrated Remediation



*Integrated Remediation Eases Work Flow Burden*

# IronPort Email Encryption

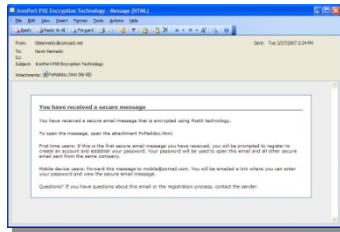
*Easy-to-Use, Easy-to-Deploy, Easy-to-Manage*



# Secure Messaging

## Email Encryption That's Easy For Receivers

### 1. Open Attachment

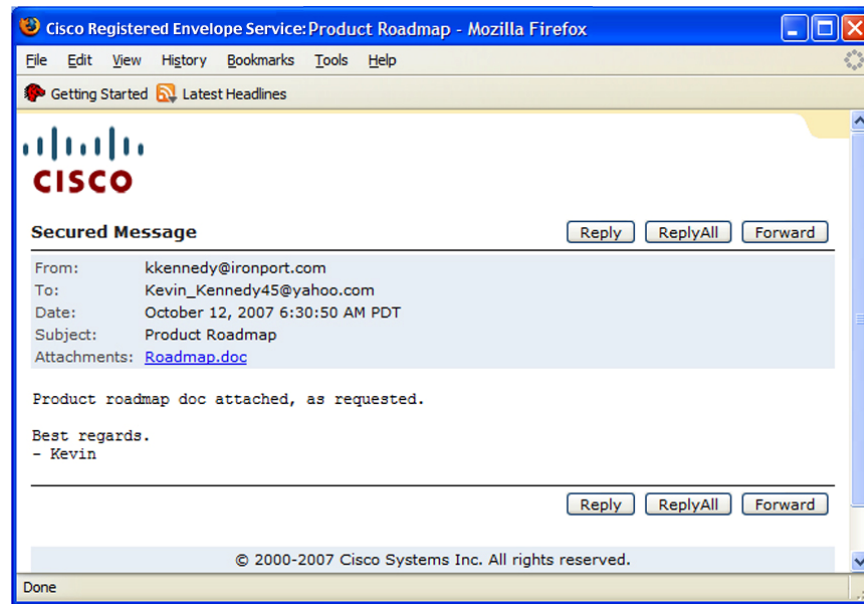


Send To Anyone  
No Certificates  
No Plug-Ins

### 2. Enter password



### 3. View message



# Enhance Visibility and Control

## Checking, Locking and Expiring Messages

The screenshot displays the Cisco Registered Email Service interface. At the top left is the Cisco logo. The top right shows a user greeting: "Welcome Schuyler Ullman" with a "Log Out" link. The main content area is titled "SEARCH SENT MESSAGES". On the left is a navigation menu with "Manage Messages" (highlighted), "Compose Message", and "Edit Profile". The search section includes a "Basic Search" tab and a "Keyword" input field with a "Search" button. Below the search bar are links for "Update Expiration For Messages" and "Lock/Unlock Message". The search results are presented in a table with columns: To, Subject, Sent, Opened, Expires, and Locked. The table contains six rows of message data. At the bottom, it says "Cisco Registered Email Service" and includes links for "Terms of Service" and "Privacy Policy" along with a copyright notice for 2001-2007 Cisco Systems Inc.

Welcome **Schuyler Ullman** [Log Out](#)

### SEARCH SENT MESSAGES

**Basic Search** [Advanced Search](#)

Keyword

*Searches To and Subject fields.*

[Update Expiration For Messages](#) | [Lock/Unlock Message](#)

<input type="checkbox"/>	To	Subject	Sent	Opened	Expires	Locked
<input type="checkbox"/>	sullman@postx.com	<a href="#">Last one</a>	08/29/2007 03:12:27 PM			
<input type="checkbox"/>	schuyler@ullman.com	<a href="#">More tests</a>	08/29/2007 03:12:13 PM		09/29/2007 03:12:51 PM	
<input type="checkbox"/>	test@garbage.com	<a href="#">Populating table</a>	08/29/2007 03:12:01 PM			
<input type="checkbox"/>	sullman@cisco.com	<a href="#">Hello again</a>	08/29/2007 03:11:44 PM		08/29/2007 03:12:51 PM	
<input type="checkbox"/>	sullman17@yahoo.com	<a href="#">Sample Envelope</a>	08/29/2007 03:11:08 PM			
<input type="checkbox"/>	sullman@ironport.com	<a href="#">Sample Envelope</a>	08/29/2007 03:10:04 PM			

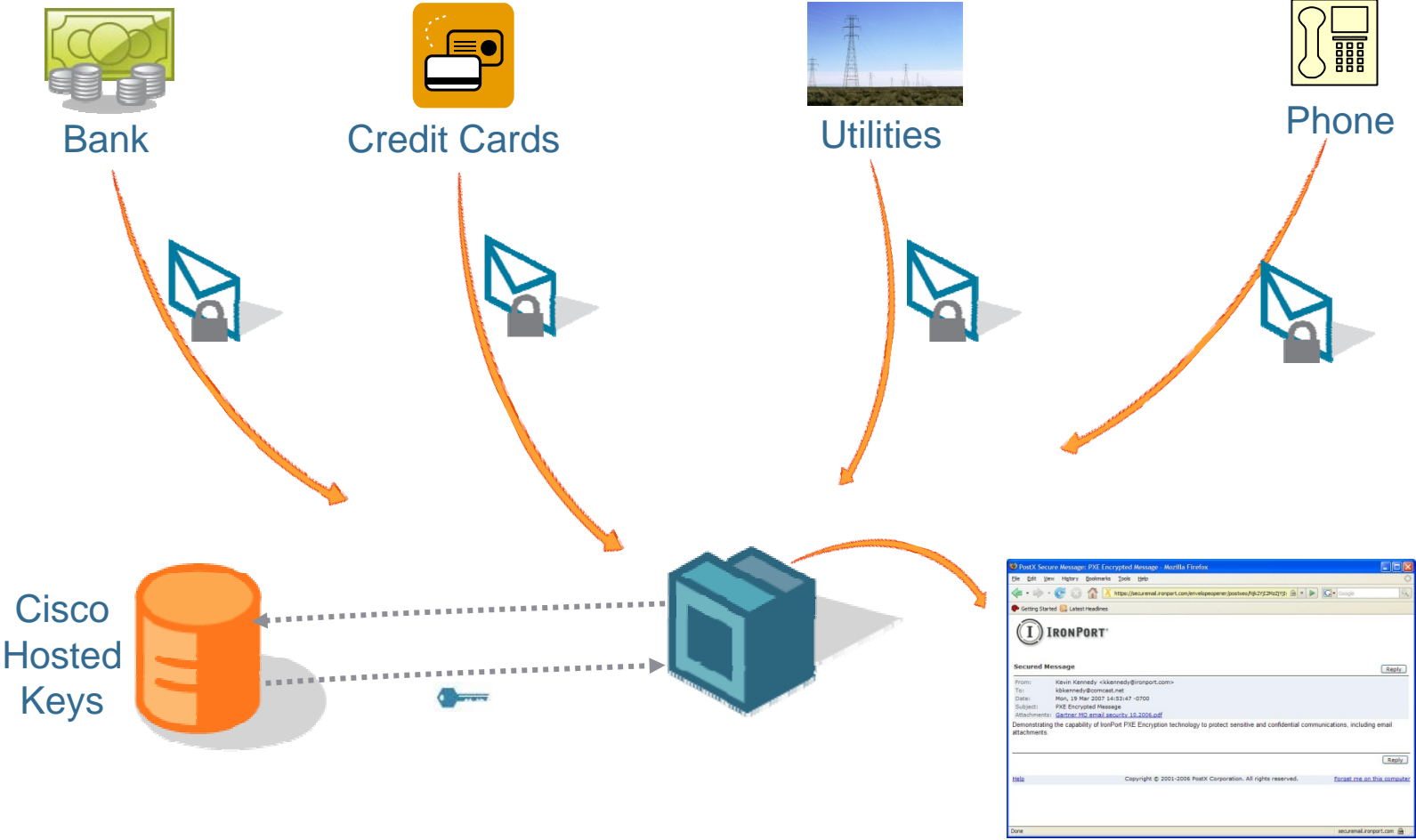
**Cisco Registered Email Service**

[Terms of Service](#) [Privacy Policy](#) © 2001-2007 Cisco Systems Inc. All rights reserved.



# Cisco Registered Envelope Service

*Single Sign-on for key process: Many Senders*



# IronPort Encryption Customer Snapshot

*Over 95% of Our Customers Use IronPort to Define Acceptable Use Policies*

Regulated Industries		Retail	All-Comers
<p><u>Financial</u></p>     	<p><u>Health Care</u></p>  <p>UnitedHealthcare®</p>   	  <p>TIFFANY &amp; CO.</p>     	<p>P I X A R</p>     <p>VERITAS</p> 

# IronPort Security Appliances

## *Integrated Security Appliances For The Network Perimeter*

- Integrated DLP Scanning and Remediation For Email
- Encryption Without any Additional Hardware Required
- Industry-leading Anti-Spam and Anti-Virus Scanning



**IronPort C-Series**  
EMAIL SECURITY APPLIANCE

- 
- Acceptable Use Policy (AUP) Management
  - Industry-leading Malware and Spyware Filtering
  - Layer 4 Traffic Monitor Inspects all Traffic



**IronPort S-Series™**  
WEB SECURITY APPLIANCE

- 
- Centralized Reporting
  - Centralized Tracking
  - Centralized Policy Management
  - Centralized Archiving



**IronPort M-Series™**  
SECURITY MANAGEMENT APPLIANCE

# Market Leadership

## Gartner

---

*IronPort Positioned in the “Leaders” Quadrant  
in Magic Quadrant Report*



---

*IronPort is positioned as a leading player in the  
messaging security appliance market*

**THE RADICATI GROUP, INC.**  
A TECHNOLOGY MARKET RESEARCH FIRM

---

*Named IronPort the market share leader  
in the email security appliance market*





THE INDUSTRY-LEADING IRONPORT C650  
EMAIL SECURITY APPLIANCE

IRONPORT C650

# TRY BEFORE YOU BUY

Sign up today and receive  
a fully-functional  
IronPort appliance  
to test in your network,  
FREE for 30 days.

 IRONPORT®

IronPort is now  
part of Cisco. 

© 2008 Cisco Systems, Inc.

95% of companies  
who try an IronPort  
appliance become  
customers.

*Contact:*

IronPort Systems,  
Thailand

Tel: 02-231-8089

[anurak@ironport.com](mailto:anurak@ironport.com)  
[anurak@cisco.com](mailto:anurak@cisco.com)





# STOP MORE. SPEND LESS.

IRONPORT. COMPREHENSIVE EMAIL SECURITY SOLUTIONS.



IronPort is now  
part of Cisco.

