Information Technology Solutions and Services

Web Traffic Monitoring

October, 1999

Patti Lawrence

Patti.Lawrence@Motorola.com

Distribution Information

This presentation contains sensitive information related to procedures in use at Motorola. You may use portions within your own Information Security organization. You may not otherwise distribute this presentation in part or in whole without written permission from Motorola.

Patti.Lawrence@Motorola.com

Why Monitor?

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Why do we need to monitor?

- Company policy for computer use
  - What is appropriate?
    - Business related activities:
      - Support Company business goals and objectives
    - Non-business related activities:
      - as approved by management
      - negligible, not interfering with work responsibilities and required business activities
      - Examples: volunteerism, continuing education, professional development

Patti.Lawrence@Motorola.com

Why do we need to monitor?

- Company policy for computer use
  - What is NOT appropriate?
    - Disclosure of confidential or sensitive data owned by or entrusted to Motorola to unauthorized recipients
    - Misuse of trademarks or service marks of Motorola or other organizations
    - Misuse of copyrighted material or other violation of copyrights held by Motorola or others

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Why do we need to monitor?

- Company policy for computer use
  - What is NOT appropriate?
    - Communicating in ways that disparage other companies' products or services (excluding objective reports of substantiated fact with limited internal distribution)
    - Communicating information that could be perceived as official Motorola positions or endorsements without proper management approval
    - Communicating using confrontational or improper language or using statements that are defamatory

Patti.Lawrence@Motorola.com

Why do we need to monitor?

- Company policy for computer use
  - What is NOT appropriate?
    - Creating, storing, or transmitting illegal or otherwise offensive material
    - Participating in any activity which could be interpreted as harassment
    - Originating or distributing chain letters
    - Misrepresenting an individual's identity or the source of communications or data

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Why do we need to monitor?

- Company policy for computer use
  - What is NOT appropriate?
    - Attempting to break into any computer ("cracking") without proper authorization, whether within Motorola or another organization
    - Accessing confidential information on computer resources without authorization
    - Promoting political or religious positions
    - Operating a personal business, or use for personal gain

Patti.Lawrence@Motorola.com

Why do we need to monitor?

- Company policy for computer use
  - What is NOT appropriate?
    - Participating or engaging in activities that violate the law, the Motorola Code of Conduct, Key Beliefs, or any Motorola policies or standards, including Human Resources, financial or security
    - Soliciting, except as provided for in the Human Resources publication “Working Together”

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Why do we need to monitor?

- Company policy for computer use
  - What is NOT appropriate?
    - Export or import of any governmentally-controlled technical data or software (such as software encryption) to or from unauthorized locations or persons without appropriate licenses or permits

10/18/99
Patti.Lawrence@Motorola.com

Why do we need to monitor?

- Network traffic
  - Before and after “normal” hours
  - Lunch time
  - Global corporation: there is ALWAYS someone trying to be productive

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Why do we need to monitor?

- Incident response (examples)
  - Insider information posted on Yahoo message boards
  - Stalker traced back to a pager number assigned to the Corporation
  - RFP competitive results and analysis disclosed to losing bidder
  - Hacking tools, software from warez sites found running on internal network

Patti.Lawrence@Motorola.com

How It All Began...

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

How It All Began...

- Posting on Yahoo message board disclosed confidential company information
- Legal department enlisted our help to find out if the posting came from within our network
- Network Security Team's RealSecure evaluation + a few Perl scripts = ad hoc system

Patti.Lawrence@Motorola.com

What We Did and Did Not Find

- Did NOT find evidence that the posting came from inside
- DID find URLs for pornographic and other inappropriate sites
- Did NOT find managers who approved this inappropriate use
- DID find outraged managers ready to deal with our findings

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

The “System” Today

Patti.Lawrence@Motorola.com

The "System" Today

- 1998 one facility
- 1999 positioned server to pick up 3 facilities
- RealSecure logs all outgoing requests to web gateway
- Weekly automated job searches through the week's logs for activity to report

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA Information Technology Solutions & Services

The "System" Today

- Weekly report of high-volume IP addresses (machines) - sample headings:

Searching pattern : . in log file: ...
Total HTTP requests: 8280520, total hits: 8280520, percentage:100%

Source IP Hits Start-End Time Stamps

Patti.Lawrence@Motorola.com

The "System" Today

- Weekly report of keyword hits on IP addresses (machines) using keywords from such categories as:
  - sex/pornography
  - racism
  - hacking/cracking
  - abuse of drugs
  - identity masking
  - etc….

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

The "System" Today

- Raw log file for each IP address in the "keyword" report
- Summary file for each address showing times of activity and counts per web server (15-minute rule)
- Counts of "hits" are added to a cumulative spreadsheet, sorted by descending cumulative total

Patti.Lawrence@Motorola.com

Tue Sep 07 08:36:28	Tue Sep 07 08:54:07	wy1fd.hotmail.msn.com	9	email	
		encrypted/unreadable	2		
		www.cucug.org	3		
		209.1.112.251	3	email	
		arc5.msn.com	3	email	
		home.netscape.com	3		
		lc2.law5.hotmail.passport.com	1	email	
		www.egreetings.com	1	greeting cards	
		www.hotmail.com	1	email	
Tue Sep 07 11:17:50	Tue Sep 07 18:38:37	www.mbusa.net	7		
		ads16.focalink.com	13		
		www.picosearch.com	1		
		209.1.112.251	3	email	
		admedia.xoom.com	25		
		www.xoom.com	7		
		classifieds.yahoo.com	1	personal ads	
		gserv.zdnet.com	1		
		personal.lycos.com	2	personal ads	
		ad.doubleclick.net	3		
		www.angelfire.com	14	user web pages	
		www.egreetings.com	148	greeting cards	
		www.hisoft.demon.co.uk	2		
		encrypted/unreadable	144		
		m.doubleclick.net	3		
		mbox.yahoo.com	3	email	
		www.snap.com	33		
		www.opera.com	6		
		a1896.g.akamaitech.net	5		
		view.avenuea.com	7		
		ads.msn.com	2	email	
		services.xoom.com	4		
		members.aol.com	6	user web pages	
		www1.bluemountain.com	33	greeting cards	

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector

MOTOROLA

Information Technology Solutions & Services

	AI	AJ	AK	AL	AM	AN	AO
3	**990905**	**990912**	**990919**	**990926**	**991003**	**991010**	**Total**
4	243	361	1583	6172	6225	0	14724
5	693	200	225	224	0	0	10068
6	0	0	0	0	0	0	9810
7	0	0	0	0	0	0	8600
8	2000	1796	850	1291	283	187	8261
9	182	409	0	0	346	304	6861
10	0	0	0	0	0	0	5315
11	894	0	0	159	572	1671	4797
12	0	0	0	0	0	0	4797
13	0	0	0	0	0	0	3864
14	656	155	0	0	0	0	3221
15	0	565	0	220	1008	0	2857
16	0	0	0	492	0	0	2700
17	0	0	0	0	276	2260	2536
18	0	0	0	0	0	0	2374
19	0	0	0	0	0	0	1877
20	0	0	0	0	0	0	1864
21	0	0	0	0	0	0	1827
22	0	0	666	0	0	0	1819
23	0	0	0	0	0	0	1807
24	167	0	0	0	0	0	1716
25	0	0	0	121	408	1126	1705
26	0	0	0	0	0	0	1582
27	0	0	0	0	0	0	1396
28	0	0	0	0	0	0	1335
29	0	0	0	0	0	0	1332
30	0	0	0	0	0	0	1315
31	0	0	131	0	473	688	1292
32	0	232	0	0	161	106	1245

Patti.Lawrence@Motorola.com

The "System" Today

- False hits analysis - samples:
  - abcnews.go.com ("teenyicon.gif")
  - accommodationsexpress.com
  - www.al-anon.alateen.org
  - www.certificationshack.com
  - www.dallasexaminer.com
  - www.flowersexpress.com
  - www.jelloboy.com ("Nude teen stick figures")

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

The "System" Today

- False hits analysis - even more samples:
  - www.JoesCrabShack.com
  - www.radioshack.com
  - www.securitiesexam.com
  - www.sunglassexpress.com
  - www.texasexes.org
  - www.uswest.net
  - xxx.lanl.gov (my favorite)

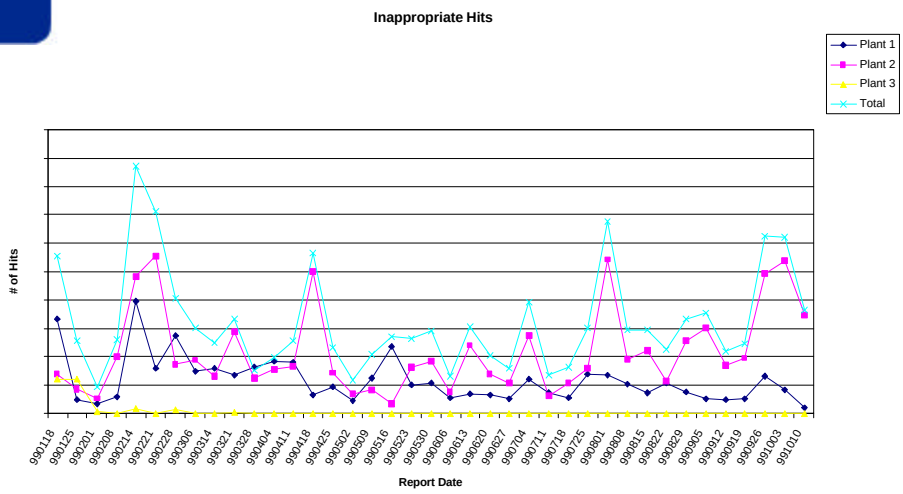
Patti.Lawrence@Motorola.com

The "System" Today

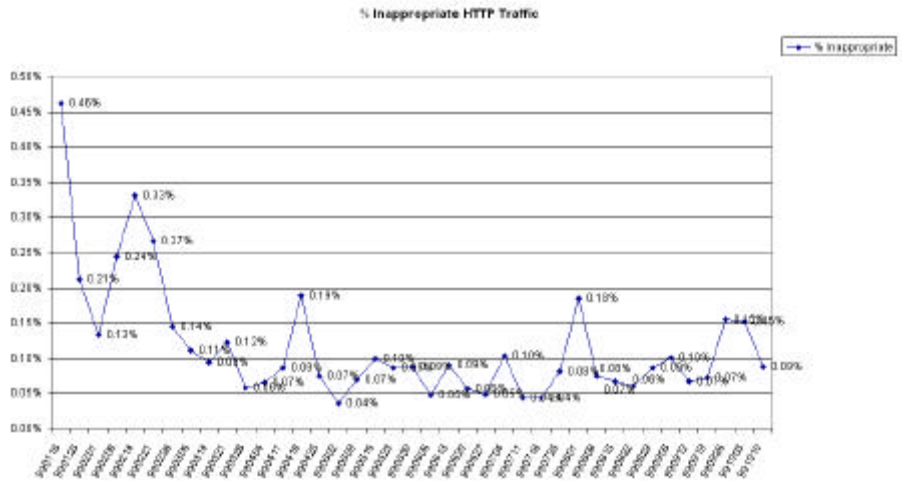
- Generate weekly summary reports and charts
  - Cover page, summary and status of open cases
  - Spreadsheets of historical data by IP address
  - Charts

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services



10/18/99
Patti.Lawrence@Motorola.com



Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

The "System" Today

- Cases opened for highest hitters, work our way down the list
- Find the computer
- Identify the user (whenever possible)
- Document the evidence using fill-in-the-blank template

Patti.Lawrence@Motorola.com

User Name:
User Network ID:
User Location:
User Department:

HR Representative:

Investigation Report Contents:

- 🖫 Electronic/Printed IP logs containing IP address of machine, count of web hits based on search criteria
- 🖫 Electronic/Printed IP logs containing IP address of machine, breakdown of web hits by site based on search criteria
- ❑ Electronic/Printed web browser history showing dates/times the sites were accessed
- ❑ Electronic/Printed cookie file from web browser
- ❑ Electronic/Printed computer security logs showing who was logged into the computer at the times in the samples
- ❑ Electronic copy of Netscape user directory
- ❑ Electronic copy of users email files (available only if stored on hard disk)
- ❑ Electronic copy of directories containing evidence
- ❑ Printed list of directories copied
- ❑ Printed examples of data found
- ❑ Statements from others involved

❑ Not Included
☒ Included
🖫 Available on request – Stored as electronic copy

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector

MOTOROLA Information Technology Solutions & Services

On {date}, weekly web traffic logs revealed the computer connected at IP address {IP address} had been to pornographic sites. The currently associated machine ID at this IP address is {machine ID}, assigned to {name or "multiple users" as appropriate}.

According to the web traffic log, at least one user on the machine connected at {IP address} has accessed pornographic sites on the dates and times reported in attached web traffic summaries.

{Choose a paragraph that fits the situation or create a similar one; delete those not; replace terms in brackets with the appropriate data}

The NT security log was reviewed for the dates and times in question. The security audit had not been turned on so there was no data in the security log. There are {number of user accounts} users on the computer, so to determine who was going to pornographic web sites we searched the cache and Netscape history files of all the users who had Netscape profiles on the machine.

The NT security log was reviewed for the dates and times in question. The security audit had not been turned on so there was no data in the security log. However, {name} was the only user on the machine.

The NT security log was reviewed for the dates and times in question. The ID shown logged in was {userID}. This ID belongs to {name}.

The Unix security log was reviewed for the dates and times in question. The ID shown logged in was {userID}. This ID belongs to {name}.

This machine is running Windows, is a portable computer, and has no security installed on it. It was in the docking station in {name}'s office, and the only Netscape profile on the machine was for {full email address for the user}.

10/18/99

Patti.Lawrence@Motorola.com

{Choose a paragraph that fits the situation or create a similar one; delete those not used; replace terms in brackets with the appropriate data}

We found that the {Netscape and/or Internet Explorer} user profile associated with the following person had been used to access pornographic sites:

Upon viewing the user's {Netscape and/or Internet Explorer} historical files, we found the following evidence the user had been to pornographic sites:

Upon viewing the user's {Netscape and/or Internet Explorer} historical files, we found no evidence this user had been to pornographic sites, indicating web activity had been cleared from the machine some time before we went to the machine for investigation on {date}.

{name}	{name of file containing evidence}	{site name} {site name} {site name} {site name}
	{name of file containing evidence}	{site name} {site name} {site name} {site name}
	{name of file containing evidence}	{site name} {site name} {site name} {site name}
	{name of file containing evidence}	{site name} {site name} {site name} {site name}

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

{Choose a paragraph that fits the situation or create a similar one; delete those not used; replace terms in brackets with the appropriate data; attach printed copy of directory listing}

The hard drive of the computer contained {number of} files consuming {amount of} disk space with pornographic data with file dates ranging from {start date/time} to {end date/time}.

The user's network home directory contained {number of} files consuming {amount of} disk space with pornographic data with file dates ranging from {start date/time} to {end date/time}.

The computer contained {executable program name} indicating the likelihood that a CD-ROM burner, jaz drive, zip drive, or other mass storage device was in use on the computer. We found {mass storage device name(s)} {in the office / attached to the machine / installed internally in the machine}.

Network Security, ITSS

Patti.Lawrence@Motorola.com

The "System" Today

- Investigation helps
  - Administrative account
  - Network access to machine
  - Security log from machine/ntlast.exe
  - Directory listings from machine
  - Web traffic logs and summaries
  - Web browser files and other files on machine
  - Files on user's network drive

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Netscape Cookies

```
www.kiss.com    FALSE  /       FALSE  1262332800      KissSearch
        PROFILEWEIGHT2=&ENDDATE=8%2F10%2F99+10%3A53%3A13+AM&PROFILEDRINK
S=&PROFILECOUNTRY=1004&PROFILERELIGION=&PICTUREFLAG=&PROFILEAGE2=&PROFI
LESEXPREF=1&PROFILEHEIGHT2=&PROFILESMOKES=&PROFILEWEIGHT1=&STARTDATE=8
%2F10%2F98&PROFILECHILDREN=&PROFILESEX=1&PROFILEAGE1=&PROFILEHEIGHT1=&S
EARCHDATE=8%2F10%2F99+10%3A53%3A13+AM
DatingClub.Com FALSE  /       FALSE  1249926908      DCVISIT         COUNT=1
DatingClub.Com FALSE  /       FALSE  1293753600      WEBTRENDS_ID    (IP deleted)-
2094752928.29287257
.imgis.com      TRUE   /       FALSE  1091543994      JEB2
        59F68616DEC19E3B88B602DE3004A518
www.loveme.com          TRUE   /       FALSE  1924992163      STRING          singlesites
.carprices.com  TRUE   /       FALSE  965860046       PARTNER         SINGLE
.carprices.com  TRUE   /       FALSE  965860046       RETURN          VISITOR
aff.carprices.com FALSE  /       FALSE  965952104       PARTNER         SINGLE
www.one-and-only.com    FALSE  /       FALSE  965951522       usergroup       0
.jobs.com       TRUE   /       FALSE  1293839999      RMID    88b602dd37b1b3c0
.snap.com       TRUE   /       FALSE  946684799       u_edition_0_0   home
.snap.com       TRUE   /       FALSE  946684799       u_vid_0_0       04a891f8
www.amcity.com FALSE  /       FALSE  1565114549      Apache  cache-engine-
03.chi.ais.net.314534934394549283
personals.yahoo.com     TRUE   /       FALSE  949359600       L
        prop=p&c0=Scottsdale&s0=AZ&z0=85252&r0=Phoenix
.amazon.com     TRUE   /       FALSE  934963200       session-id-time 934963200
.amazon.com     TRUE   /       FALSE  934963200       session-id      002-9419992-6572637
.amazon.com     TRUE   /       FALSE  2082787304      ubid-main       002-4511810-3623549
```


Patti.Lawrence@Motorola.com

Netscape Preferences

```
user_pref("browser.bookmark_columns_win", "v1 1 1:10000 2:2996 4:1999 3:1999");
user_pref("browser.bookmark_window_rect", "132,132,929,729");
user_pref("browser.cache.disk_cache_size", 15000);
user_pref("browser.cache.memory_cache_size", 15000);
user_pref("browser.download_directory", "D:\\Download\\");
user_pref("browser.link_expiration", 120);
user_pref("browser.print_background", true);
user_pref("browser.startup.homepage", "http://sstg.geg.mot.com");
user_pref("browser.startup.homepage_override", false);
user_pref("browser.url_history.URL_1", "www.yam.ch/");
user_pref("browser.url_history.URL_10", "www.msnbc.com/");
user_pref("browser.url_history.URL_11", "www.egreetings.com/");
user_pref("browser.url_history.URL_12", "g:\\apps\\cidm\\fa_sys\\f3fillw\\f3fillw2.exe");
user_pref("browser.url_history.URL_13", "g:\\\\apps\\cidm\\fa_sys\\f3fillw\\f3fillw2.exe %1");
user_pref("browser.url_history.URL_14", "\\\\hy-fs1\\vol1\\apps\\cidm\\fa_sys\\f3fillw\\f3fillw2.exe %1");
user_pref("browser.url_history.URL_15", "http://wms.geg.mot.com/");
user_pref("browser.url_history.URL_2", "profiles.yahoo.com/");
user_pref("browser.url_history.URL_3", "http://www.linuxjournal.com");
user_pref("browser.url_history.URL_4", "http://www.mfsoft.com");
user_pref("browser.url_history.URL_5", "www.arizonarepublic.com/");
user_pref("browser.url_history.URL_6", "www.azrepublic.com");
user_pref("browser.url_history.URL_7", "www.uswest.com/");
user_pref("browser.url_history.URL_8", "www.uswestdex.com/");
user_pref("browser.url_history.URL_9", "http://www.uswest.com/");
```


Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Developing Relationships

Developing Relationships

- Human Resource Management
  - Help set priorities
  - Deal with user and his/her management
  - Apply disciplinary measures
  - I never have to confront the users and usually could not identify them if I saw them

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Developing Relationships

- Corporate Legal Department
  - Issues involving software licensing (freeware vs. shareware, etc.)
  - Sometimes initiate investigation request
  - Assist with decisions regarding evidence storage and retention, etc.

Patti.Lawrence@Motorola.com

Developing Relationships

- Physical Security Department
  - Liaison with local, state, and federal law enforcement when required
  - Need to be informed if evidence suggests the possibility of bodily harm or destruction of property
  - Place cameras when a “public” machine does not indicate who was using it

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Developing Relationships

- Law Enforcement
  - Notification of suspected illegal activity
    - Avoid changing anything on the machine (preservation of evidence)
    - Provide technical expertise in interpreting evidence (especially with local-level agencies)

Patti.Lawrence@Motorola.com

Developing Relationships

- Network Architecture Team
  - Locate a machine when inaccessible over the network
  - Provide access to network services not normally required

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Lessons Learned

Patti.Lawrence@Motorola.com

Lessons Learned

- UNIX limitations
  - when trying to parse the data the Unix operating system (Solaris 2.6) can not handle a file size larger then 2GB. This required daily generation of a new log file and combining all at the end of the week
  - Tabling output in procedures resulted in over 40 files being open at a time

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Lessons Learned

- RealSecure limitations
  - Version we are using has a memory leak, requiring us to start/stop process on an hourly basis to avoid loss of data
  - This is an older version of the software, and no longer being maintained
  - Newer versions don’t work with our processes

Lessons Learned

- Network limitations
  - We had to add two new network segments to support the Real Secure engine, which could not handle ATM.
  - We had to dual-homed the system to the monitored network and the "out of band" network used to pull the data off the system because the level of 2-way traffic caused network traffic problems (packet collisions)

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Lessons Learned

- People issues
  - Habits and Impressions --> Increased activity
    - “They haven’t caught me yet”
    - “They aren’t downsizing right now”
  - Need to raise policy awareness level
    - orientation of new employees and contractors
    - reminders to existing employees and contractors
  - Manager reaction: “Now I understand why there was a productivity problem…”

Patti.Lawrence@Motorola.com

Lessons Learned

- People issues
  - Creative surfing
    - "Glare screens"
    - Non-standard web browsers
    - Web sites that don't hit keywords
    - Remote access surfing
  - If you can't identify who is on the machine, try searching the log for web-based email!

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Plans for the Future

Plans for the Future

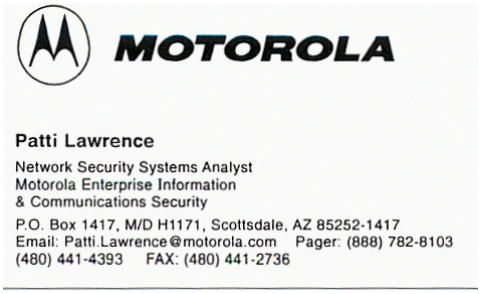
- Evaluate, test, implement filtering software
- Continue monitoring
  - Some things will slip through filtering software
  - We expect continued historical-evidence requests outside scope of filtering software
- Automate everything that can be automated
- Analyze keywords for possible changes
- Cover more facilities/business units

Patti.Lawrence@Motorola.com

Commercial Government Industrial Solutions Sector
MOTOROLA
Information Technology Solutions & Services

Questions, Comments, Suggestions...

Patti.Lawrence@Motorola.com


MOTOROLA
Patti Lawrence
Network Security Systems Analyst
Motorola Enterprise Information
& Communications Security
P.O. Box 1417, M/D H1171, Scottsdale, AZ 85252-1417
Email: Patti.Lawrence@motorola.com Pager: (888) 782-8103
(480) 441-4393 FAX: (480) 441-2736