



## Technology Workshop **Is your Technology Secure?**

September 26, 2013

Microsoft®  
Small Business  
Specialist

**Microsoft®**  
**CERTIFIED**  
*Partner*



# Welcome!

---

- Thank you for joining us today.
- In today's call we will cover a few tips and tricks to help you get your technology more secure. We'll wrap up by 1pm.
- If you want to follow from your office, go to [www.ekaru.com](http://www.ekaru.com) / Go to "What's New" near the bottom of the page. Presentation will open in a browser, click the down arrow in nav bar to advance slides.

# Format

- Given the number of people on the line today, this is a “listen only” call.
  - (Reason, cut down on ambient noise, avoid “call on hold music” – a bit tough though, because I can’t hear you!)
- If you have questions, please eMail to [knoran@ekaru.com](mailto:knoran@ekaru.com) and we will try to include Q&A at the end of the call – we will be reviewing email live during the call.
- Call 978-692-4200 for help.



# Workshop Mission

---

- Help you get more from the technology you already have.
- Introduce you to new technologies you need to know about.

# Topics

---

- The **Massachusetts Data Security Law** went into effect three years ago. Are you aware of all the rules?
- Are your systems up to date with **security patches**?
- Why does **antivirus software** require so many updates?
- Are **all** the computers on your network safe?
- Is your **backup** up to date?

# Security in the news...

---

Microsoft Patch Tuesday brings critical Explorer, Outlook fixes

Update Flash, Shockwave ASAP!  
Adobe also patches Acrobat and Reader

## 'Master key' to Android phones uncovered

A "master key" that could give cyber-thieves unfettered access to almost any Android phone has been discovered by security



# What's in it for you?

---

- GOAL: PROTECT your business
- Ekaru provides managed services to monitor your network/systems
- We always advise clients to know *enough* so they feel secure (we can worry about the details for you)

# Massachusetts Data Security Law

---

- Applies to all businesses
- Your industry may have additional requirements (HIPAA, etc)



# Technology requirement #1

1. **“Secure user authentication protocols including:**
  - (a) control of user IDs and other identifiers;
  - (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
  - (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
  - (d) restricting access to active users and active user accounts only; and
  - (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;”

# ... Technology Requirement #1

- *Strong Passwords include 8 or more characters, include uppercase letters, lowercase letters, numbers, and symbols. Never use a word in the dictionary.*
  - *GOOGLE: Microsoft Strong Password Checker.... You can actually see the strength of the password grow with increased character types, etc.*
- *90 Day Password Policy.*
- *Domain authentication should be used for businesses with a server.*
- *"Technically feasible" – not all applications have password policies*

# Technology requirement #2

- **“Secure access control measures that:**
- (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
- (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;”

# Technology requirement #3

- “(3)Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.”
- *Do not email personal information. Instead use encrypted email or encrypted file transfer.*
- *Maintain wireless network encryption.*
- *WPA NOT WEP Encryption*
- *Password protection is NOT encryption!*

# eMail Encryption

- Sign up for a free trial at <http://voltage.ekaru.com/>

**Voltage security** | **SecureMail Cloud™** | **Ekaru** contact [cloud login](#)

[home](#) | [demo](#) | [trial](#) | [subscribe](#) | [quick start](#) | [faq](#)

### On-Demand Encryption

Rapid and cost-effective options to secure collaboration with business partners and clients

- ▶ Rapid project ramp up and get going fast
- ▶ Lowest cost on-demand service
- ▶ Minimized IT overhead
- ▶ Full integration with on-premise solution
- ▶ Email, Files and Documents protected wherever they go

[View the Voltage SecureMail experience ▶](#)

### Easy to Use Email, File and Document Encryption

Protect client confidentiality with easy to use, on-demand email, file and document encryption

- ▶ Designed for Business Professionals
- ▶ Easy to use, no setup required
- ▶ No software and no purchase needed for recipients
- ▶ Integrates with Microsoft Office 2007
- ▶ Low cost subscription

[View the Voltage SecureFile experience ▶](#)

### SecureMail Cloud Demo

See how users experience SecureMail Cloud

[Click to View](#)



### Free Trial

Try Voltage SecureMail Cloud for 30 days

[Click to Try](#) **FREE**



# Technology requirement #4

---

- “Reasonable monitoring of systems, for unauthorized use of or access to personal information”;

# EventLog Analyzer

---

- Server logs can be checked for unauthorized access
- Reporting tools make review easier:

# EventLog Analyzer

## Top Hosts with Failed Logons

Host	Event Count
No Data available for the selected time period from 2012-10-30 13:11:00 to 2012-11-29 12:11:00	

## Top Users with Successful Logins

User	Event Count
User 1 (Example user names for demonstration)	37436
User 2	17339
User 3	10158
User 4	9505
User 5	8541
User 6	7944
User 7	7357
User 8	6661
User 9	6091
User 10	5529

## Top Users by Failed Logins

User	Event Count
No Data available for the selected time period from 2012-10-30 13:11:00 to 2012-11-29 12:11:00	

## Top Users with Successful Interactive Logins

User	Event Count
Admin 1	28
Admin 2	2



# Technology requirement #5

- “Encryption of all personal information stored on laptops or *other portable devices*\*;”
- *We recommend TrueCrypt or PGP encryption to mount encrypted drives. We do not recommend full disk encryption. Education is needed to ensure users don't copy files to unencrypted areas.*

\* *If technically feasible*

# Technology Requirement #5

- Do all portable devices need to be encrypted? - YES – whenever technically feasible. Also, DVDs and flash drives should be encrypted.
- Laptops: PGP or Truecrypt – You MUST remember your encryption key!



# Technology requirement #6

- “For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date **firewall protection** and operating **system security patches**, reasonably designed to maintain the integrity of the personal information.”

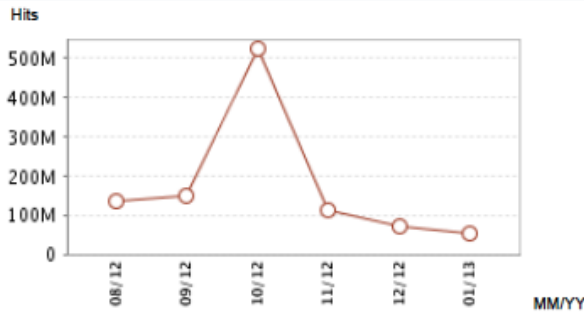
# Firewall / Firmware Updates

Name	Serial Number	Product Line	Firmware	Support
Company 1	Serial # Suppressed	TZ 105W	5.8.1.6	12/21/2013 0:00
Company 2	Serial # Suppressed	TZ 200 Domestic	5.8.1.8	2/17/2015 0:00
Company 3	Serial # Suppressed	TZ 100W	5.8.1.8	10/5/2013 0:00
Company 4	Serial # Suppressed	TZ 210	5.8.1.9	3/26/2013 0:00
Company 5	Serial # Suppressed	TZ 210	5.8.1.9	3/27/2013 0:00
Company 6	Serial # Suppressed	TZ 105	5.8.1.6e	1/25/2014 0:00
Company 7	Serial # Suppressed	TZ 200 Domestic	5.6.0.11	9/18/2014 0:00
Company 8	Serial # Suppressed	TZ 200 Domestic	5.5.1.0e	5/2/2013 0:00
Company 9	Serial # Suppressed	TZ 100	5.8.1.8	4/10/2013 0:00
Company 10	Serial # Suppressed	TZ 100	5.8.0.3	6/15/2014 0:00
Company 11	Serial # Suppressed	TZ 105W	5.8.1.6	12/7/2013 0:00
Company 12	Serial # Suppressed	TZ 100	5.8.0.3	6/15/2014 0:00

# Perimeter – Intrusion Prevention

## Viruses Blocked

Over Time: Last 6 Months

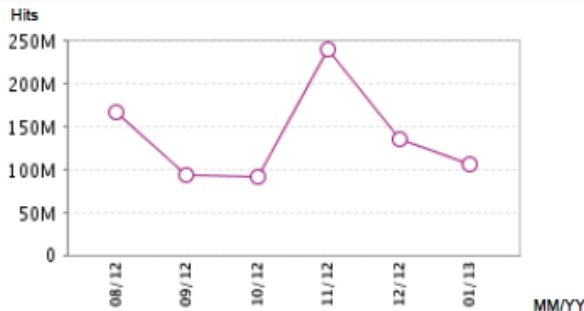


Top Viruses Blocked

Virus Name	Percentage of Viruses
Prosti.C_6	39%
Happy_3	17%
Medpinch.A#mp3	4%
Suspicious#frame	4%
Generic.Shellcode.1	3%
Suspicious#waledac.6	1%
SWF.J	1%
Elderado.B	0.9%
Morto.A_3	0.8%
Perelett.14919	0.8%

## Intrusions Prevented

Over Time: Last 6 Months



Top Intrusions Prevented

Intrusion Name	Percentage of Intrusions
Microsoft SMB2 Negotiate Reque...	13%
Ramnit C&C Traffic	7%
SIP Stress Test Traffic 1a	5%
Client Application Shellcode E...	5%
UltraVNC Client Buffer Overflo...	4%
Suspicious Javascript Code 1	4%
HTTP Server Directory Traversa...	3%
Suspicious TFTP Traffic 6	3%
DECLARE EXEC Statement 2 (Poss...	2%
SIP Stress Test Traffic 12 (3...	2%

# Perimeter Security

The screenshot shows the SonicWall Network Security Appliance interface. The left sidebar contains navigation options: WAN Acceleration, Log (selected), View, Categories, Syslog, Automation, Flow Reporting, Name Resolution, Reports, and ViewPoint. The main area displays a 'Log View' table with the following data:

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	02/27/2013 10:19:31.720	Error	Network Access	Web site access denied			Category:6 -	
2	02/27/2013 10:07:53.448	Error	Network Access	Web site access denied			Category:4 -	
3	02/27/2013 10:01:06.896	Error	Network Access	Web site access denied			Category:4 -	
4	02/27/2013 09:57:54.448	Error	Network Access	Web site access denied			Category:4 -	

Details removed for privacy

# Technology requirement #7

- “Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.”

# Managed Service

Desktop	Logged On User	Operating System	Available	Antivirus	MalwareBytes	Free Disk Space	S.M.A.R.T	Security Updates	Critical Updates	Third Party Patch
A		Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
B		Windows Vista (TM) Ultimate 6.0	■	■	■	■	■	■	■	■
C		Windows 7 Professional 6.1	■	■	■	■	■	■	■	■
C	User	Windows 7 Home Premium 6.1	■	■	■	■	■	■	■	■
E		Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
F		Windows Vista (TM) Business 6.0	■	■	■	■	■	■	■	■
G	User	Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
H	User	Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
I		Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
J	User	Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
K		Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
L	User	Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
M		Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
N	User	Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
O		Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
P		Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
Q	User	Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
R		Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
S		Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
T		Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
U	User	Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
V		Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
W	USer	Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
X		Microsoft Windows XP 5.1	■	■	■	■	■	■	■	■
Y	User	Windows 7 Professional 6.1	■	■	■	■	■	■	■	■
Z	User	Windows 7 Professional 6.1	■	■	■	■	■	■	■	■



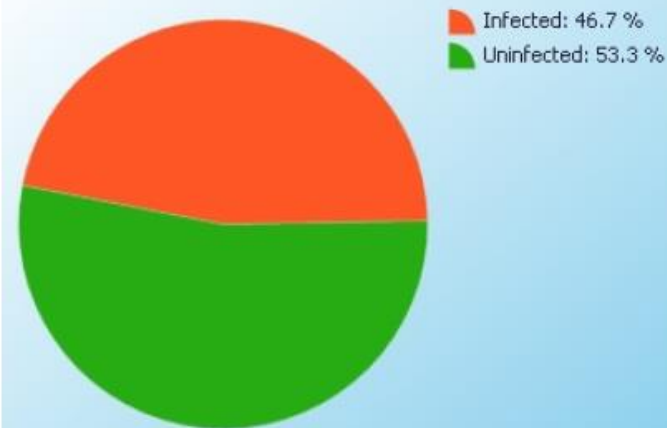
# Antivirus Report

## Executive Summary

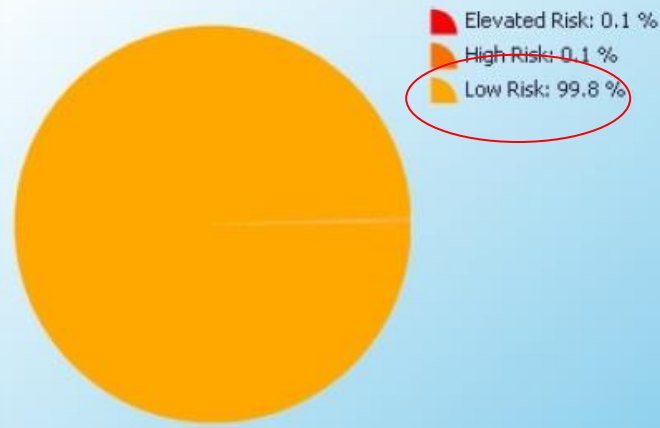


Report contains data from 1/1/2013 through 2/1/2013

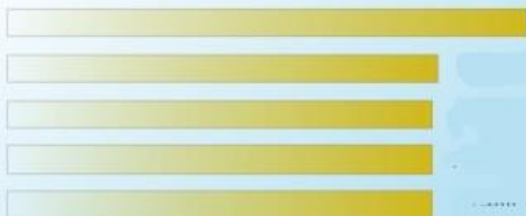
### Infected vs. Uninfected Scans



### Severity of Threats Found



### Top 10 Infected Machines



### Top 10 Threats Found



Cookie: Tracking Cookies : 2  
Malware: 15, Cookies (15) : 1

# Technology requirement #8

- “Education and training of employees on the proper use of the computer security system and the importance of personal information security.”
- *Users often break basic rules for “convenience”. Education is needed to prevent this.*
- Risk analysis is an ongoing process

# Steps to Compliance

## – Phased Approach

---

- Information audit – what data do you have and where is it?
- Review current security policies/procedures with respect to new requirements
- Identify areas for remediation
- Fix the weaknesses wherever technologically feasible
- WRITE IT DOWN! – Written Information Security Policy (WISP)

# “Patch Tuesday”

- Day the Microsoft releases security patches for all products.
- Second Tuesday of the month

[Security TechCenter](#) > [Security Bulletins](#) > [Microsoft Security Bulletin Summary for September 2013](#)

## Microsoft Security Bulletin Summary for September 2013

Published: Tuesday, September 10, 2013

**Version:** 1.0

This bulletin summary lists security bulletins released for September 2013.

# “Patch Tuesday”

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Affected Software
MS13-067	<p><b>Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2834052)</b></p> <p>This security update resolves one publicly disclosed vulnerability and nine privately reported vulnerabilities in Microsoft Office Server software. The most severe vulnerability could allow remote code execution in the context of the W3WP service account if an attacker sends specially crafted content to the affected server.</p>	Critical Remote Code Execution	May require restart	Microsoft Office, Microsoft Server Software
MS13-068	<p><b>Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (2756473)</b></p> <p>This security update resolves a privately reported vulnerability in Microsoft Outlook. The vulnerability could allow remote code execution if a user opens or previews a specially crafted email message using an affected edition of Microsoft Outlook. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.</p>	Critical Remote Code Execution	May require restart	Microsoft Office
MS13-069	<p><b>Cumulative Security Update for Internet Explorer (2870699)</b></p> <p>This security update resolves ten privately reported vulnerabilities in Internet Explorer. The most severe vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited the most severe of these vulnerabilities could gain the same user rights as the current user. Users whose accounts are configured to have fewer user</p>	Critical Remote Code Execution	Requires restart	Microsoft Windows, Internet Explorer

# Support ends for Windows XP

Desktop operating systems	Latest service pack	End of extended support
<b>Windows XP</b>	<b><u><a href="#">Service Pack 3</a></u></b>	<b><u><a href="#">April 8, 2014</a></u></b>
Windows Vista	<u><a href="#">Service Pack 2</a></u>	April 11, 2017
Windows 7 *	<u><a href="#">Service Pack 1</a></u>	January 14, 2020
Windows 8	Not yet available	January 10, 2023

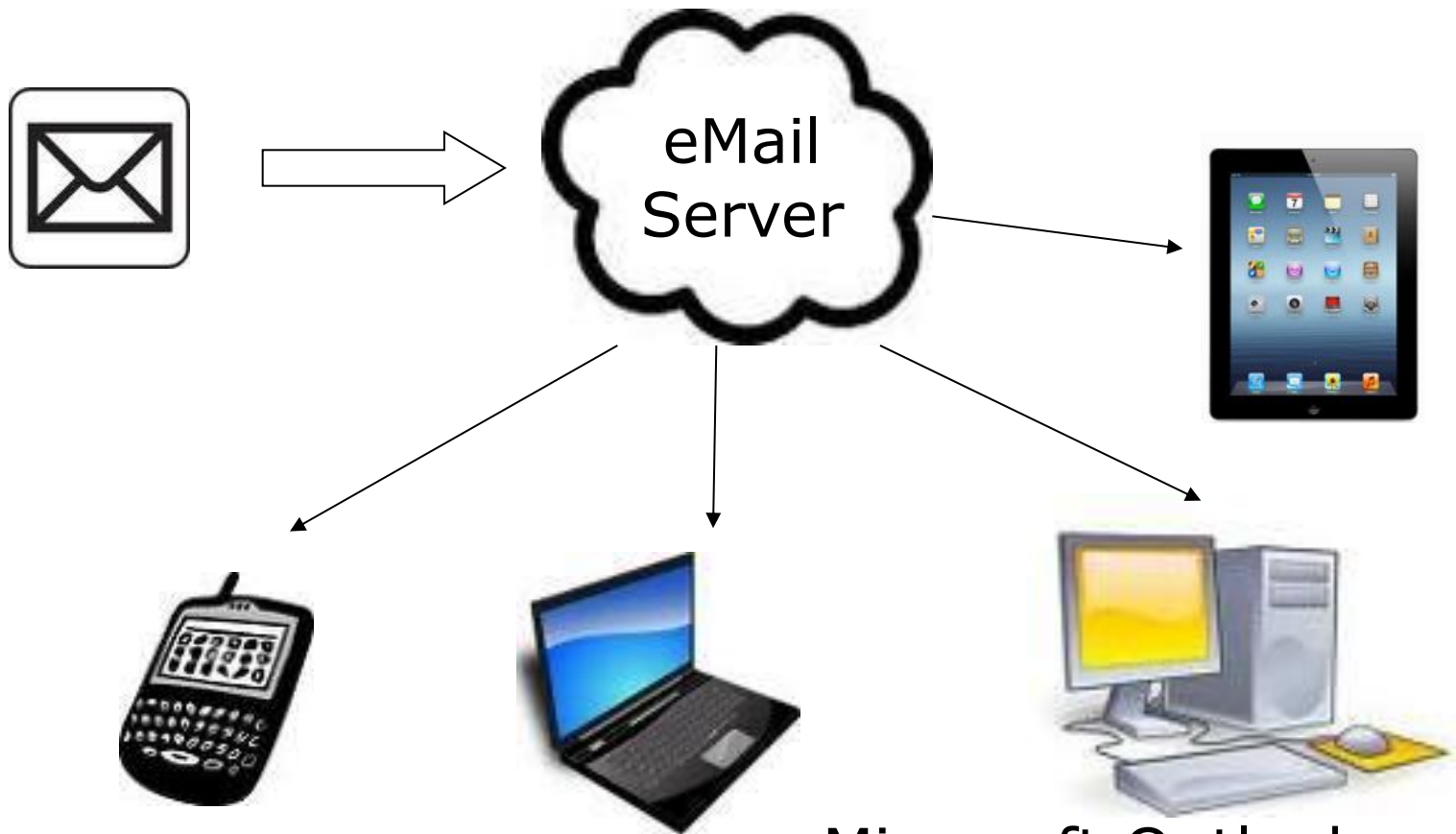
***Start planning now if you have Windows XP systems***

# Windows XP... planning

---

- As a general rule, we don't recommend updating just the operating systems for PCs older than three years old.
- Best solution in most cases is a replacement PC

# Where is your mail?

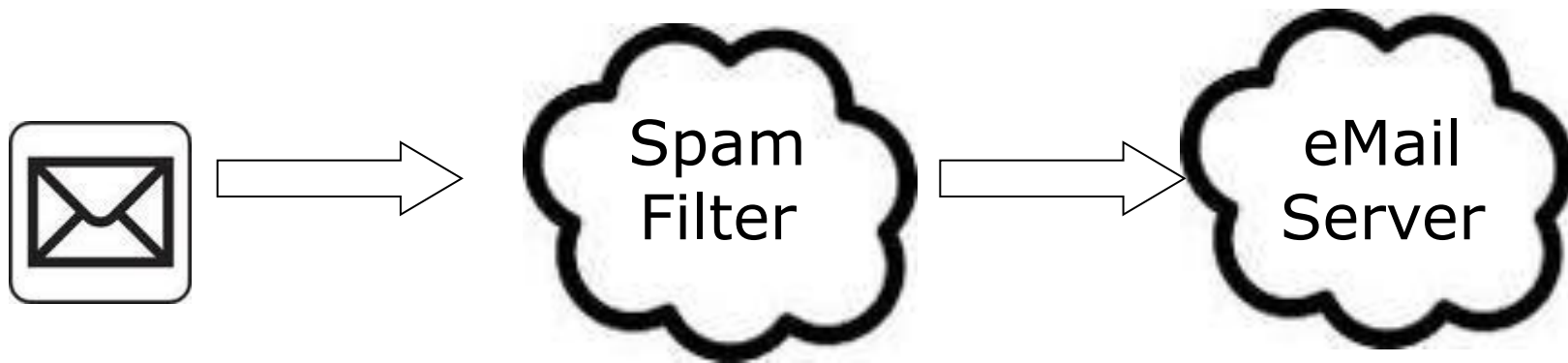


- Microsoft Outlook
- WebMail





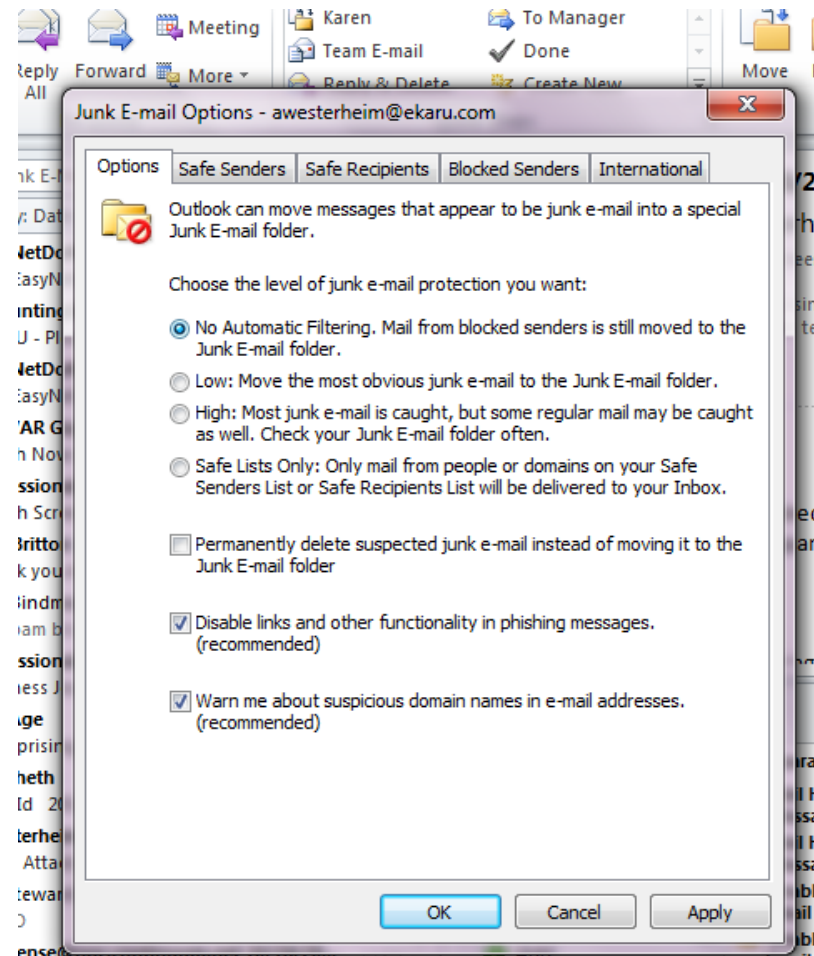
# Clear the clutter! – Spam!



- Filter Spam BEFORE it gets to your mail server!
- For some customers, filtering 30,000 spam messages a month! – **90% of total email volume**
- First step to organization is to control spam!

# Use ONE Junk Filter

- Turn off your Outlook Junk filter if you use another tool.
- Watch out – Re-install Office may re-set the settings.
- We recommend NOT using Outlook Junk and instead using “Cloud” filtering.



# eMail + Passcode

- If employees use email on their phones, passcodes are a **MUST**



# Mobile Data?

---

- What is your company policy on mobile data?
- What are you doing about “BYOD” – Bring Your Own Device to work?

# Antivirus Updates - Monitored

System / Day	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
SRV1	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
SRV2	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

*Monitoring shows that each server received an antivirus update every day of the month as planned.*

# “Third Party” Patching

---

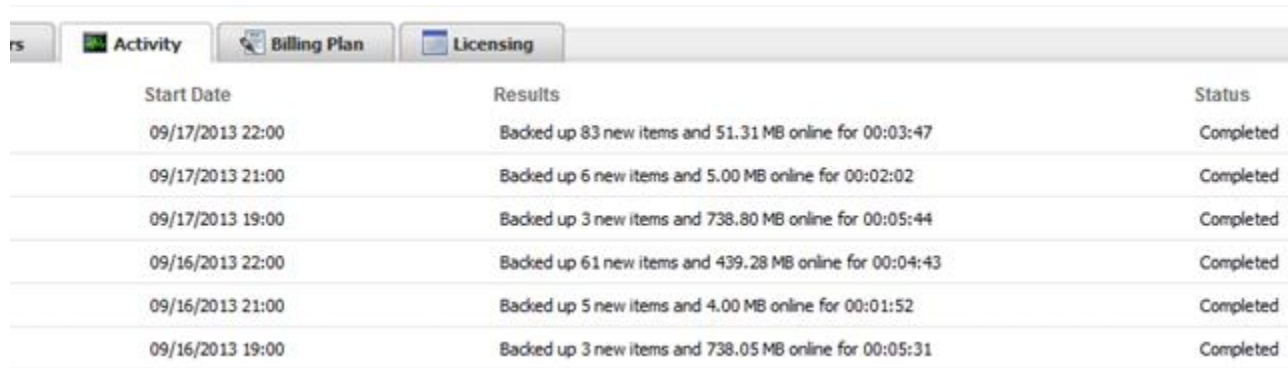
- Adobe Acrobat
- Adobe AIR
- Adobe Flash Player
- Adobe Reader
- Adobe Shockwave Player
- Apple iTunes
- QuickTime
- Mozilla Firefox
- Java Development Kit
- Java Runtime Environment

# Patch Schedule

---

- Release (“Patch Tuesday” for Microsoft – Security & Critical Patches)
- Test (up to 48 hours / 2 weeks)
- Schedule
- Deploy
- *REBOOT*

# Backup monitoring



The screenshot shows a web interface with three tabs: 'Activity', 'Billing Plan', and 'Licensing'. The 'Activity' tab is selected, displaying a table of backup operations. The table has three columns: 'Start Date', 'Results', and 'Status'. All entries in the table show a 'Completed' status.

Start Date	Results	Status
09/17/2013 22:00	Backed up 83 new items and 51.31 MB online for 00:03:47	Completed
09/17/2013 21:00	Backed up 6 new items and 5.00 MB online for 00:02:02	Completed
09/17/2013 19:00	Backed up 3 new items and 738.80 MB online for 00:05:44	Completed
09/16/2013 22:00	Backed up 61 new items and 439.28 MB online for 00:04:43	Completed
09/16/2013 21:00	Backed up 5 new items and 4.00 MB online for 00:01:52	Completed
09/16/2013 19:00	Backed up 3 new items and 738.05 MB online for 00:05:31	Completed

- Is the backup occurring on schedule?
- Are ALL critical files being backed up?



# Backup and Disaster Recovery

---

- Full image
- Virtual machine in the event of a server failure
- “Cloud” virtualization in the event of a site catastrophe

# Backup and Disaster Recovery

Site Name	Friendly Name	Agent Type	Agent Provisioned On	Device Name	Volume (s) Backed Up	Backup Interval (In Minutes)	ONSITE						OFFSITE					
							Last Backup Date / Time	Last Backup Status	Incremental Size (MB)	Total Space Used (GB)	Alerts	Screen hot Verification of Backup	Connect to Device	Last Backup Date / Time	Live Data set (GB)	Total Space Used (GB)	Alerts	Connect to Cloud
SITE	SRV 1	Server Vault Pro	8/16/2013 1:29 PM	SRV 1	C, D	30	9/19/2013 10:34 AM	✓	418.73	313.64	✓	✓	✓	9/17/2013 9:33 AM	290.97	340.88	✓	☰ → ☁
	SRV 2	Desktop Vault Pro	8/16/2013 1:20 PM	SRV 2	C	30	9/19/2013 10:31 AM	✓	37.23	41.50	✓	✓	✓	9/19/2013 9:31 AM	33.12	53.95	✓	☰ → ☁

Total No. Of Vault(s) : 2

- What level of protection do you need?
- Balance with budget requirements

# Security Re-Cap

- Antivirus up to date?
- Anti-Malware up to date?
- Security patches up to date?
- Backup up to date?
- *If you do everything "right", you can still have a problem, but your chances are much lower.*
- eMail us with questions or if you want more detailed instructions: [info@ekaru.com](mailto:info@ekaru.com)



# Thank You!:

---

For more information:

**Ekaru**  
*Connecting People with Technology*  
978-692-4200  
[www.ekaru.com](http://www.ekaru.com)

Sign up for Ekaru's free Technology Advisor e-newsletter