Ekaru Connecting People With Technology

Technology Workshop
HIPAA – Security Risk Assessments

November 25, 2013

Microsoft Small Business Specialist

Microsoft CERTIFIED Partner

Welcome!

- Thank you for joining us today.
- In today's call we'll cover the Security Assessment and next steps.
- If you want to follow from your office, go to 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 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 your practice understand what is needed to complete your security assessment and related documentation
- Save you time in the process

These materials do not constitute legal advice and are for educational purposes only. The information in this webinar is based on current federal law and subject to change based on changes in federal law, the effect of state law or subsequent interpretative guidance.

Security Risk Assessment

- Reminder for Assessments:

For those of you participating in the Meaningful Use Program, it is necessary to complete a security risk assessment as part of your attestation.

If this is your second year of meaningful use, your risk assessment will need to be completed by December 31, 2013.

An information security risk assessment involves identifying and assessing risks to confidentiality, integrity and availability of patient information within your location. This not only applies to computer based systems, but also any paper records that contain personally identifiable health information.

HITECH

- The **Health Information Technology for Economic and Clinical Health (HITECH)** Act provides the **Department of Health & Human Services (HHS)** with the authority to establish programs to improve health care quality, safety, and efficiency through the promotion of health IT, including electronic health records and private and secure electronic health information exchange.

  Under HITECH, eligible health care professionals and hospitals can qualify for Medicare and Medicaid incentive payments when they adopt certified EHR technology and use it to achieve specified objectives.

Meaningful Use

Stage 1	Stage 2	Stage 3
2011-2012	**2014**	**2016**
Data capture and sharing	Advance clinical processes	Improved outcomes

Stage 1: Meaningful use criteria focus on:	Stage 2: Meaningful use criteria focus on:	Stage 3: Meaningful use criteria focus on:
Electronically capturing health information in a standardized format	More rigorous health information exchange (HIE)	Improving quality, safety, and efficiency, leading to improved health outcomes
Using that information to track key clinical conditions	Increased requirements for e-prescribing and incorporating lab results	Decision support for national high-priority conditions
Communicating that information for care coordination processes	Electronic transmission of patient care summaries across multiple settings	Patient access to self-management tools
Initiating the reporting of clinical quality measures and public health information	More patient-controlled data	Access to comprehensive patient data through patient-centered HIE
Using information to engage patients and their families in their care		Improving population health

Next Steps

- Complete the Security Risk Analysis
- Remediate gaps
- Complete/update your documentation

Myths…

From HealthIT.gov

- **The security risk analysis is optional for small providers.**

False. All providers who are "covered entities" under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.

- **Simply installing a certified EHR fulfills the security risk analysis MU requirement**.

False. Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR. …

Myths…

- **My EHR vendor took care of everything I need to do about privacy and security.**

False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.

- **My security risk analysis only needs to look at my EHR**.

False. Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone).

Myths…

- **I only need to do a risk analysis once.**

False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections.

Understanding the Basics

- **Source: American Medical Association – Toolkit:** http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act.page

- HIPAA privacy and security toolkit: Helping your practice meet new compliance requirements – **OUTSTANDING RESOURCE!**
- HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information
- Sample Notice of Privacy Practices
- Sample Business Associate Agreement

Source: HIPAA privacy and security toolkit

- http://www.ama-assn.org//resources/doc/washington/hipaa-toolkit.pdf
- 25 Pages long
- Includes 11 “How to HIPAA” tips

HIPAA Privacy and Security Toolkit

1. Basics
2. Compliance Requirements
3. Prioritize Compliance Requirements
4. Privacy Notice
5. Breach Notification
6. Business Associate Agreements
7. HIPAA Security Rule
8. Patients Rights
9. Limit Disclosures to Minimum Necessary
10. Penalties
11. AMA Website Resources

Source: HIPAA privacy and security toolkit

- HIPAA = Health Insurance Portability and Accountability Act
- Privacy, Security, and Breach Notification Requirements
- HITECH = Health Information Technology for Economic and Clinical Health Act
- Violations result in serious penalties

Requirements

- Physicians should also note that HIPAA is considered a “floor,”. States such as Massachusetts have requirements that go above and beyond what the federal government requires. (**MA Data Security Law**)

Privacy Rule

- Restricts "covered entities" and "business associates" use of Protected Health Information (PHI)
- "Business Associates" include people or companies hired to help your practice including accountants, billing services, lawyers, and consultants.

Privacy Rule

- "Protected health information" = individually identifiable information that is held or transmitted by a covered entity or business associate in any form or media (electronic, paper, or oral) that relates to the past, present, or future physical or mental health of an individual, health care services, or payment for health care

Privacy Rule

- "The Privacy Rule also provides for "individual rights" such as a patient's right to access their PHI, restrict disclosures, request amendments or an accounting of disclosures and their right to complain without retaliation"

Security Rule

- The **Security Rule** requires covered physician practices to implement "administrative, technical, and physical safeguards" to ensure the confidentiality, integrity, and availability of *electronic* PHI.
- "Electronic PHI or *e*PHI" refers to all individually identifiable health information a covered entity or business associate creates, receives, maintains or transmits in electronic form.

Breach Notification

- The **Breach Notification Rule** requires covered physician practices to notify affected individuals, the Secretary of the U.S. Department of Health & Human Services (HHS) and, in some cases, the media when they discover a breach of a patient's unsecured PHI.
- Proper use of **encryption** can help avoid these notification requirements

Encryption

- Mitigate breach notification requirements if data is encrypted.
- Encryption is NOT the same as password protection
- eMail – like sending a postcard – NOT secure (use encrypted mail)

- REFERENCE – AMA HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information.

Compliance Deadline

- September 23, 2013
  - Most obligations took effect years ago.
  - Advised to re-evaluate plans regularly (new business associations, new practices, new technology, etc)
  - Requires periodic review of technical and non-technical requirements
  - New technical requirements with HITECH act.

Government Audits

- HHS Office of Civil Rights "OCR" has established a an audit protocol.
- 170 potential audit areas
- Available on-line: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

Government Audits

Rule
vities &
nplaint

Check All | Uncheck All

Export as CSV | Export as XML

All (169) Security (78) Privacy (81) Breach (10)

Show All entries

Search: Clear

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification	HIPAA Compliance Area
§164.308	§164.308(a)(1): **Security Management Process §164.308(a)(1)(ii)(a)** - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity,...	Conduct Risk Assessment	Inquire of management as to whether formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and avail...	Required	Security
§164.308	§164.308(a)(1)(i): **Security**	Acquire IT Systems and Services	Inquire of management as to whether formal or	Required	Security

Must have formal documentation

Preparation: Security Risk Assessment

Ekaru Connecting People With Technology

Security Risk Assessment

Completed by
Date Completed

Item number	Type	Security Rule	Implementation Specifications	Team	Required / Addressable	Risk Assessment Question	Responsibility	Risk Assessment	Policy	Comments (Action items / Assigned to)	Location in Policy Guidance Document
1	Administrative Safeguards	Security Management Process 164.308(a)(1)	Risk Analysis	Security Official, Physician, Workforce Members	Required	Does any vendor have access to confidential patient data? Have you discussed HIPAA Security and HITECH requirements with such vendor(s)? Is an up-to-date Business Associate Agreement in place for each vendor that has access to ePHI?	Emerson IS Dept. and Practice				
2	Administrative Safeguards	Security Management Process 164.308(a)(1)	Risk Analysis	Security Official, Physician, Workforce Members	Required	Can a vendor change confidential patient data? If so, are you monitoring audit logs for such changes?	Emerson IS Dept. and Practice				
3	Administrative Safeguards	Security Management Process 164.308(a)(1)	Risk Management	Security Official, Physician, Workforce Members	Required	Do you update your workforce members' training each time you develop and implement new policies and procedures? Do you document initial and continuing training?	Emerson IS Dept. and Practice				
4	Administrative Safeguards	Security Management Process 164.308(a)(1)	Risk Management	Security Official, Physician, Workforce Members	Required	Have you set user access to ePHI that corresponds to job function?	Emerson IS Dept. and Practice				
5	Administrative Safeguards	Security Management Process 164.308(a)(1)	Risk Management	Security Official, Physician, Workforce Members	Required	Do you monitor reports that identify persons and systems that access ePHI, including those not authorized to have access to ePHI?	Emerson IS Dept. and Practice				

135+ Line Items to Review!

Microsoft Small Business Specialist

Microsoft CERTIFIED Partner

Security Risk Assessment

- Administrative, Physical, Technical, Breach Notification
- Security Rule is referenced
- Risk Analysis, Risk Management, Protection from Malicious software, Password management, Backup, etc.
- "Required" or "Addressable"
- Responsibility: Hospital IS vs. Practice
- Risk Assessment: No Risk, Possible Risk, Risk
- Policy / Location in Policy Document

Security Risk Assessment

- Many practices completed this last year
- Re-Visit responses – Have you addressed risks properly?
- Documentation – do you have proper documentation?

Conduct a Gap Analysis

- Policies and Procedures – Is your documentation current?
- Have you taken all steps feasible to reduce the risk of breach?

Security Requirements

- Are you using your IT system's log-in process to authorize access (such as limiting administrative access)?
- Have you implemented a security awareness and training program for all members of your workforce, including management?
- Have you installed anti-virus and other anti-malware protection software on your computers? Do you use it to guard against, detect, and report any malicious software? Do you protect against spyware?

Significant Penalties

- Civil Penalties:

HIPAA Violation	Penalty Range	Annual Maximum
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 - $50,000 per violation	$1.5 million
Individual "knew, or by exercising reasonable diligence would have known" of the violation, but did not act with willful neglect	$1,000 - $50,000 per violation	$1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 - $50,000 per violation	$1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation	$1.5 million

Significant Penalties

- Criminal Penalties:
  - Covered entities and specified individuals whom "knowingly" obtain or disclose individually identifiable health information in violation of the HIPAA requirements face a fine of up to $50,000, as well as imprisonment up to one year.
  - Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison.
  - Offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years.

Technology Requirements

- Physicians should also note that HIPAA is considered a "floor,". States such as Massachusetts have requirements that go above and beyond what the federal government requires. (**MA Data Security Law**)

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

Massachusetts Data Security Law

- Applies to *all* businesses
- Personal Information = First Name + Last Name or First Initial + Last Name and any personal identifying information
- SPECIFIC technology requirements

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/

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.*
- *Full disk Encryption*
- *Hardware encryption if available*

* *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!

Smart Phones

- iPhone Encryption: http://support.apple.com/kb/ht4175

Data protection is available for devices that offer hardware encryption, including iPhone 3GS and later, all iPad models, and iPod touch (3rd generation and later). Data protection enhances the built-in hardware encryption by protecting the hardware encryption keys with your passcode. This provides an additional layer of protection for your email messages attachments, and third-party applications.

iPhone Encryption

Enable data protection by configuring a passcode for your device:

- Tap **Settings > General > Passcode**.
- Follow the prompts to create a passcode.
- After the passcode is set, scroll down to the bottom of the screen and verify that "Data protection is enabled" is visible.

- **Passcode tips**
- Use these passcode settings to maximize passcode security:
- Set Require Passcode to Immediately.
- Disable Simple Passcode to use longer, alphanumeric passcodes.
- Enable Erase Data to automatically erase the device after ten failed passcode attempts.

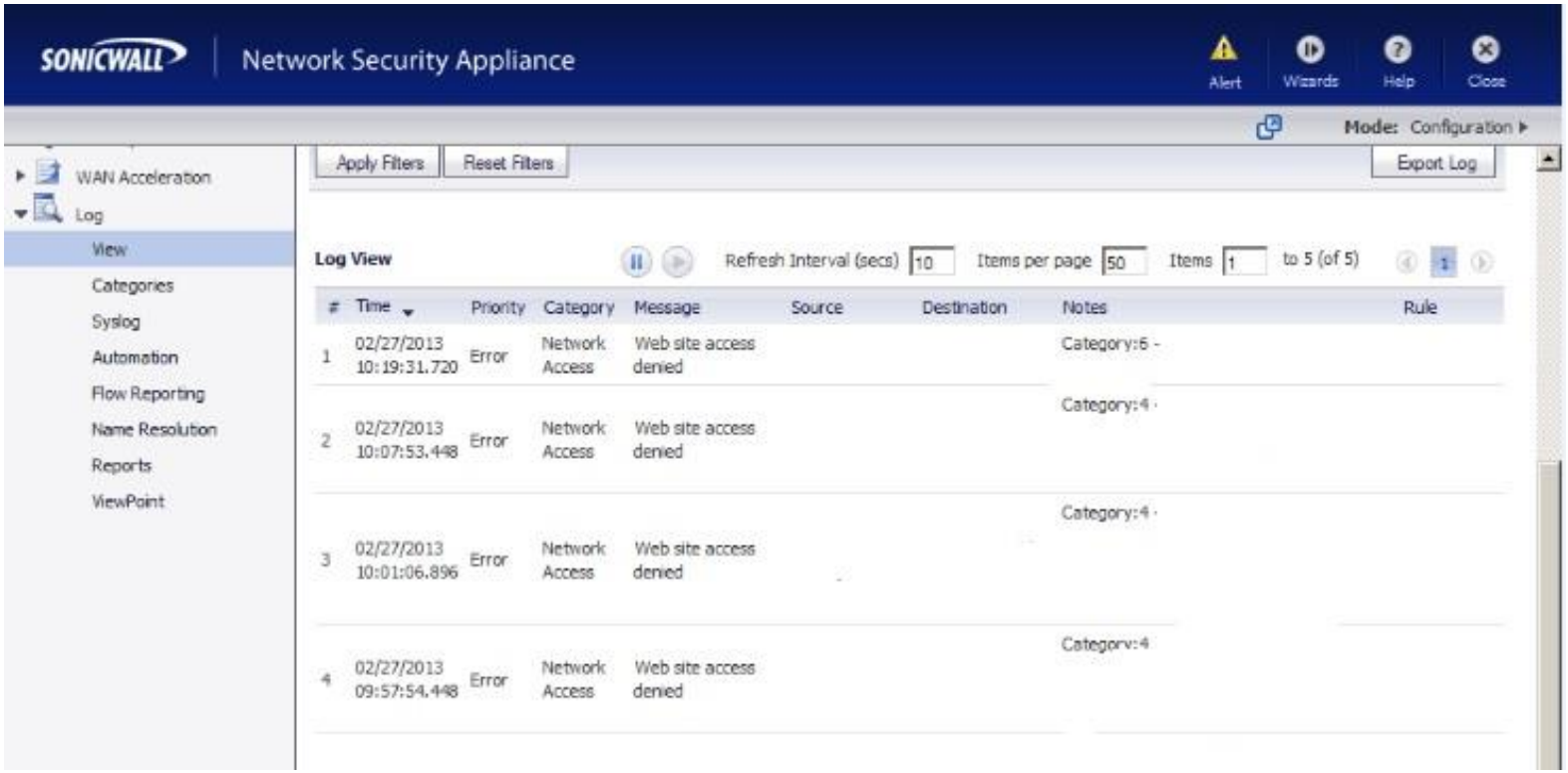
Technology requirement #6

- "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 Security



Details removed for privacy

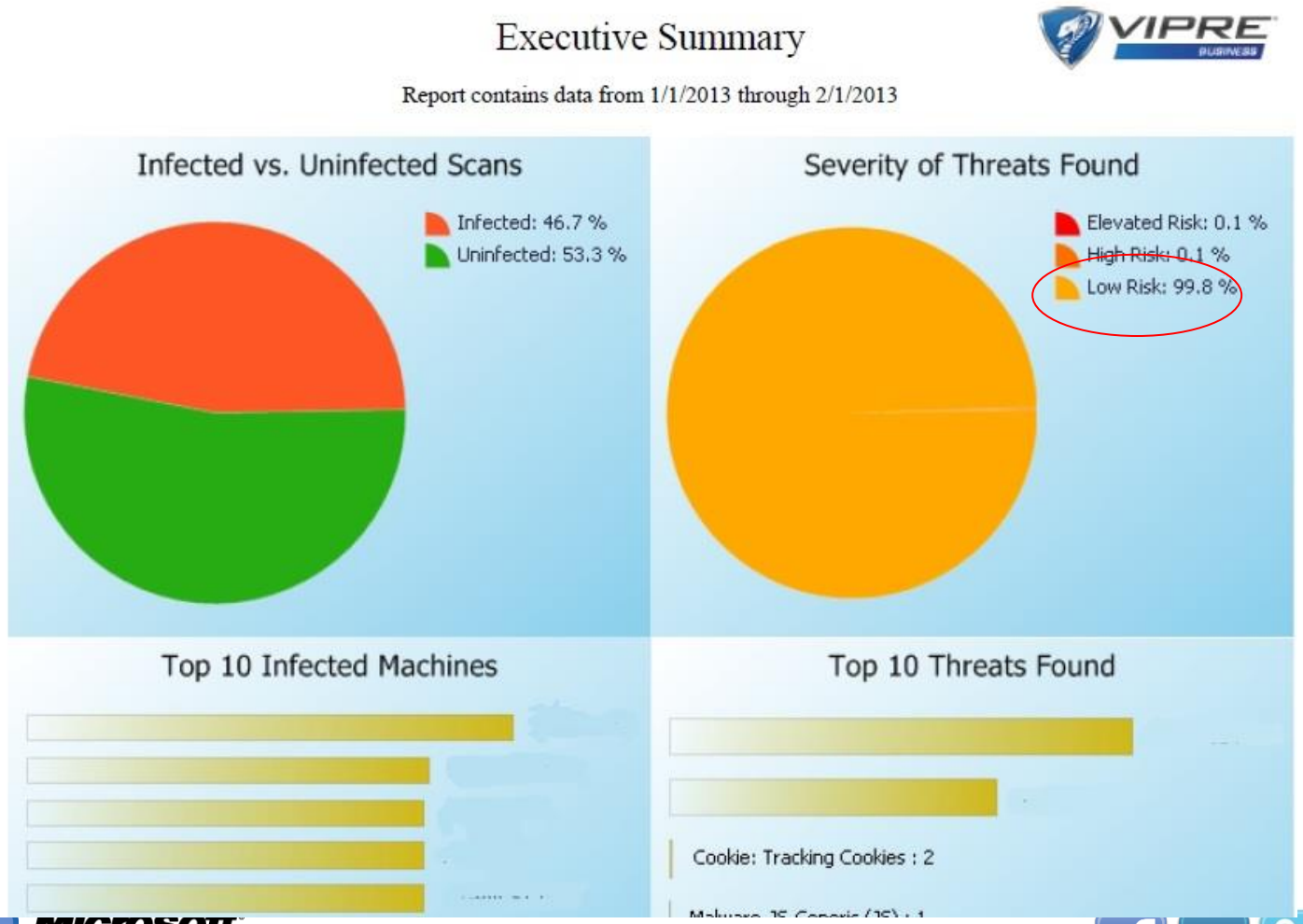
Technology requirement #7

- ”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



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

"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	**Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2834052)** 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.	Critical Remote Code Execution	May require restart	Microsoft Office, Microsoft Server Software
MS13-068	**Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (2756473)** 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.	Critical Remote Code Execution	May require restart	Microsoft Office
MS13-069	**Cumulative Security Update for Internet Explorer (2870699)** 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	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
Windows XP	**Service Pack 3**	**April 8, 2014**
Windows Vista	Service Pack 2	April 11, 2017
Windows 7 *	Service Pack 1	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

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.

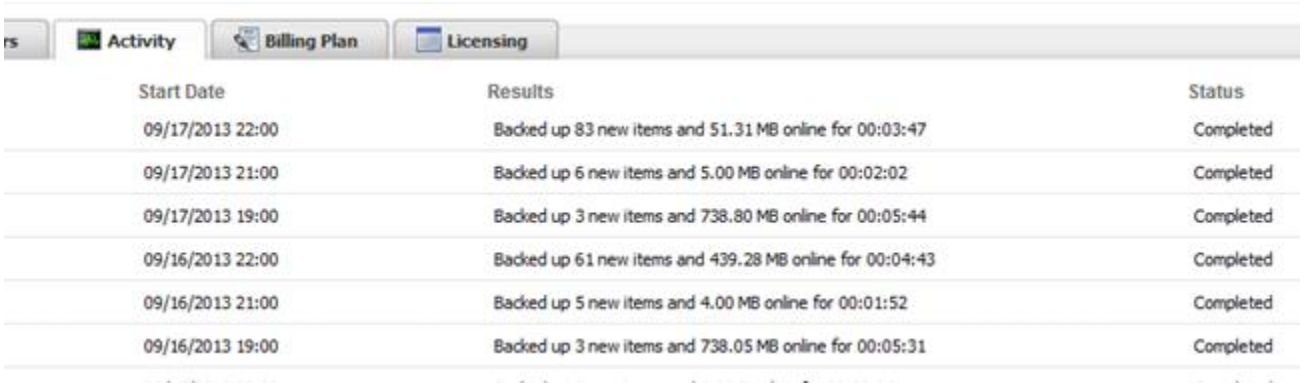
"Third Party" Patching

- 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



- 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	Screenshot Verification of Backup	Connect to Device	Last Backup Date / Time	Live Dataset (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

Summary

- Leverage on-line resources
- Most of what you need to do, you're already doing
- Don't be intimidated by "buzz words" – ask us!
- Everything has to be documented
- … but don't re-invent the wheel
- **There is no such thing as 100% security**

Next Steps

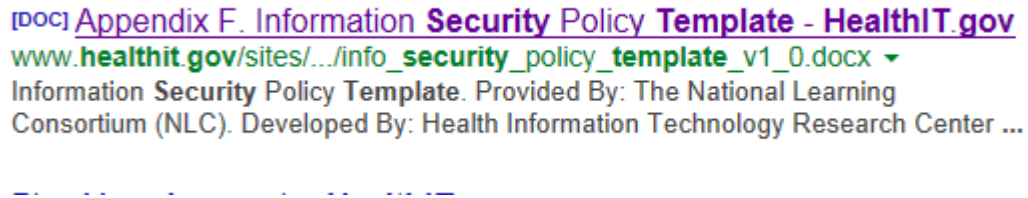
- Complete the Security Risk Analysis
- Remediate gaps / have a plan
- Complete/update your documentation

Additional Resources

- HealthIT.gov - http://www.healthit.gov/providers-professionals/ehr-privacy-security/10-step-plan
- HealthIT.gov - http://www.healthit.gov/providers-professionals/top-10-myths-security-risk-analysis

Documentation

1. HealthIT.gov: Security Policy Template


[DOC] Appendix F. Information **Security** Policy **Template** - **HealthIT.gov**
www.**healthit.gov**/sites/.../info_**security**_policy_**template**_v1_0.docx
Information **Security** Policy **Template**. Provided By: The National Learning Consortium (NLC). Developed By: Health Information Technology Research Center ...

2. http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act.page
   - Sample Notice of Privacy Practices
3. - Sample Business Associate Agreement

Thank You!:

For more information or
to schedule a security assessment:

Ekaru
Connecting People with Technology
978-692-4200
www.ekaru.com

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