Technology Workshop
HIPAA – Security Risk Assessments

November 25, 2013
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

<table>
<thead>
<tr>
<th>Stage 1</th>
<th>Stage 2</th>
<th>Stage 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2011-2012</strong></td>
<td><strong>2014</strong></td>
<td><strong>2016</strong></td>
</tr>
<tr>
<td>Data capture and sharing</td>
<td>Advance clinical processes</td>
<td>Improved outcomes</td>
</tr>
</tbody>
</table>

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

- 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

- 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”
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 ePHI" 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)

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 an audit protocol.
- 170 potential audit areas
Government Audits

<table>
<thead>
<tr>
<th>Rule</th>
<th>Check All</th>
<th>Uncheck All</th>
<th>Export as CSV</th>
<th>Export as XML</th>
</tr>
</thead>
<tbody>
<tr>
<td>All (169)</td>
<td>Security (78)</td>
<td>Privacy (81)</td>
<td>Breach (10)</td>
<td></td>
</tr>
</tbody>
</table>

### Section: §164.308
#### Established Performance Criteria
- §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, and availability...

#### Key Activity
- Conduct Risk Assessment
- Acquire IT Systems and Services

#### Audit Procedures
- 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 availability...

#### Implementation Specification
- Required

#### HIPAA Compliance Area
- Security

Must have formal documentation
## Preparation:
**Security Risk Assessment**

### Security Risk Assessment

<table>
<thead>
<tr>
<th>Item number</th>
<th>Type</th>
<th>Security Rule</th>
<th>Implementation Specifications</th>
<th>Team</th>
<th>Required / Addressable</th>
<th>Risk Assessment Question</th>
<th>Responsibility</th>
<th>Risk Assessment</th>
<th>Policy</th>
<th>Comments (Action items / Assigned to)</th>
<th>Location in Policy Guidance Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Administrative Safeguards</td>
<td>Security Management Process 164.308(a)(1)</td>
<td>Risk Analysis</td>
<td>Security Official, Physician, Workforce Members</td>
<td>Required</td>
<td>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?</td>
<td>Emerson IS Dept. and Practice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Administrative Safeguards</td>
<td>Security Management Process 164.308(a)(1)</td>
<td>Risk Analysis</td>
<td>Security Official, Physician, Workforce Members</td>
<td>Required</td>
<td>Can a vendor change confidential patient data? If so, are you monitoring audit logs for such changes?</td>
<td>Emerson IS Dept. and Practice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Administrative Safeguards</td>
<td>Security Management Process 164.308(a)(1)</td>
<td>Risk Management</td>
<td>Security Official, Physician, Workforce Members</td>
<td>Required</td>
<td>Do you update your workforce members’ training each time you develop and implement new policies and procedures? Do you document initial and continuing training?</td>
<td>Emerson IS Dept. and Practice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Administrative Safeguards</td>
<td>Security Management Process 164.308(a)(1)</td>
<td>Risk Management</td>
<td>Security Official, Physician, Workforce Members</td>
<td>Required</td>
<td>Have you set user access to ePHI that corresponds to job function?</td>
<td>Emerson IS Dept. and Practice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Administrative Safeguards</td>
<td>Security Management Process 164.308(a)(1)</td>
<td>Risk Management</td>
<td>Security Official, Physician, Workforce Members</td>
<td>Required</td>
<td>Do you monitor reports that identify persons and systems that access ePHI, including those not authorized to have access to ePHI?</td>
<td>Emerson IS Dept. and Practice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

135+ Line Items to Review!
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:

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

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
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 Logins

<table>
<thead>
<tr>
<th>Host</th>
<th>Event Count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*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

<table>
<thead>
<tr>
<th>User</th>
<th>Event Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>User 1 (Example user names for demonstration)</td>
<td>37436</td>
</tr>
<tr>
<td>User 2</td>
<td>17339</td>
</tr>
<tr>
<td>User 3</td>
<td>10158</td>
</tr>
<tr>
<td>User 4</td>
<td>9505</td>
</tr>
<tr>
<td>User 5</td>
<td>8541</td>
</tr>
<tr>
<td>User 6</td>
<td>7944</td>
</tr>
<tr>
<td>User 7</td>
<td>7357</td>
</tr>
<tr>
<td>User 8</td>
<td>6661</td>
</tr>
<tr>
<td>User 9</td>
<td>6091</td>
</tr>
<tr>
<td>User 10</td>
<td>5529</td>
</tr>
</tbody>
</table>

#### Top Users by Failed Logins

<table>
<thead>
<tr>
<th>User</th>
<th>Event Count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*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

<table>
<thead>
<tr>
<th>User</th>
<th>Event Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin 1</td>
<td>28</td>
</tr>
<tr>
<td>Admin 2</td>
<td>2</td>
</tr>
</tbody>
</table>
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!

**TRUECRYPT**
FREE OPEN-SOURCE ON-THE-FLY ENCRYPTION

Home Documentation Downloads News Future History Screenshots Donations
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.
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, alphanumerical 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

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>Windows Vista (TM) Ultimate 6.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td>Windows 7 Professional 6.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>User</td>
<td>Windows 7 Home Premium 6.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td></td>
<td>Windows Vista (TM) Business 6.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>J</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>O</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>W</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>User</td>
<td>Microsoft Windows XP 5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>User</td>
<td>Windows 7 Professional 6.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Z</td>
<td>User</td>
<td>Windows 7 Professional 6.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Antivirus Report

Executive Summary

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

Infected vs. Uninfected Scans

- Infected: 46.7%
- Uninfected: 53.3%

Severity of Threats Found

- Elevated Risk: 0.1%
- High Risk: 0.1%
- Low Risk: 99.8%

Top 10 Infected Machines

Top 10 Threats Found

- Cookie: Tracking Cookies: 2
- Malware & Crypto (E): 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
“Patch Tuesday”

- Day the Microsoft releases security patches for all products.
- Second Tuesday of the month
## “Patch Tuesday”

<table>
<thead>
<tr>
<th>Bulletin ID</th>
<th>Bulletin Title and Executive Summary</th>
<th>Maximum Severity Rating and Vulnerability Impact</th>
<th>Restart Requirement</th>
<th>Affected Software</th>
</tr>
</thead>
</table>
| 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 rights on the system could be less impacted than users who operate with administrative user rights. | Critical Remote Code Execution | Requires restart | Microsoft Windows, Internet Explorer |
## Support ends for Windows XP

<table>
<thead>
<tr>
<th>Desktop operating systems</th>
<th>Latest service pack</th>
<th>End of extended support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows XP</strong></td>
<td><strong>Service Pack 3</strong></td>
<td><strong>April 8, 2014</strong></td>
</tr>
<tr>
<td>Windows Vista</td>
<td><strong>Service Pack 2</strong></td>
<td>April 11, 2017</td>
</tr>
<tr>
<td>Windows 7 *</td>
<td><strong>Service Pack 1</strong></td>
<td>January 14, 2020</td>
</tr>
<tr>
<td>Windows 8</td>
<td>Not yet available</td>
<td>January 10, 2023</td>
</tr>
</tbody>
</table>

*Start planning now if you have Windows XP systems*
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

- 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

Documentation

1. ▶ HealthIT.gov: Security Policy Template


2. • 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