Reducing Risk for Small Provider Practices

Lee Kim

Director, Privacy and Security

HIMSS North America

September 6, 2017

HIMSS
transforming health through IT

HIMSS Initiatives

- HIMSS Privacy & Security Committee
- HIMSS Healthcare Cybersecurity Community
- Advocacy and public policy (examples)
  - NIST Cybersecurity Framework
  - National Cyber Incident Response Plan
- Awareness initiatives
  - 4th year of privacy & cyber awareness activities
- Information sharing
  - Monthly cyber reports

HIMSS
transforming health through IT

Privacy & Security for Small Practices

- Small practices should adopt an efficient, streamlined approach to cybersecurity.
- Acceptable use policies w/ do's & don't's
- Privacy policy should accurately reflect what the practice does (or does not do) with patient information
- Policies and procedures should be tailored to what the practice actually does (not just "boilerplate").
- Awareness training and reminders can help reduce the risk associated with the human element of security.

Privacy & Security for Small Practices: Staying Ahead of the Threat

- There is no such thing as a 100% secure solution!
- Cyber-attacks and compromises happen frequently.
- The threat is external (hackers) & internal (insider threat actors: unintentional & malicious insiders)
- Thus, we have to *block* what we can and *tackle* what we can.
- Practices should have security policies, procedures, and sanctions in place.
- Practices should regularly assess and manage risk.

Privacy & Security for Small Practices: Potential Cyber-Attacks

- Your practice may be compromised by ransomware, a denial of service attack, credential stealing malware, or an attacker who has stolen password hashes or other credentials.
- Reactive security is calling your consultant (or attorney) after a breach and addressing the aftermath.
- Proactive security is taking positive steps to prevent and mitigate threats.
- Try not to be low hanging fruit for the cyber-attacker by **not** monitoring your systems & networks, etc.

Privacy & Security for Small Practices: Potential Cyber-Attacks

- How an attacker may compromise your machine:
  - Open SMB ports & other open ports
  - Buffer overflow attacks
  - Disabling or bypassing anti-virus software
  - Encoded or encrypted shellcode
  - Weak, defeat, or repeat passwords; stolen password hashes
  - Port and traffic redirection
  - Compromised websites & VPNs
  - Compromised third parties

Privacy & Security for Small Practices: Potential Cyber-Attacks

- How an attacker may compromise your machine (cont.):
  - Web application attacks (e.g., XSS, SQLi)
  - Using your network management tools/SW/OS
  - Uploading hacking tools to your machine
  - Unpatched or outdated systems
  - Old or outdated web server software
  - Exploitation of a system process (running as system, admin, or root), etc.
  - Privilege escalation of a low priv. account

Privacy & Security for Small Practices: Cyber Defense

- Regularly conduct your risk assessments.
- Monitor your systems and networks for unusual system activity, processes, users, ports (or port usage), unusual network traffic, file integrity, etc.
- Regularly patch and update your systems (including web and mobile).
- Practice defense in-depth.
- Conduct regular awareness training programs.
- If you see something, say something. The problem might not just “go away.”

Helpful Resources

- HIMSS Healthcare Cybersecurity Community
- HIMSS privacy and security blog posts
- HIMSS Privacy and Security Toolkits
- HIMSS Privacy and Security Awareness Pages
- 2017 HIMSS Cybersecurity Survey
- HIMSS Code Red Podcast
- FBI Ransomware On the Rise
- InfraGard Cyber Health Working Group

Questions?

Lee Kim, JD, CISSP, CIPP/US

Director of Privacy and Security

lkim@himss.org