LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Healthcare Information Security Assessment and Auditing

05/28/2020

Report #: 202005281030

Agenda

- Introduction
- Information Security Assessment
- The Importance of Information Security Assessment
- Security Assessment Steps
- Security Testing
- Business Associate Agreement
- Penetration Testing
- IT Audit
- Security Assessment, Testing and Audit post Covid-19
- References
- Questions

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Introduction

- The COVID-19 pandemic has necessitated an increase in information collection and sharing among providers, patients, hospitals, vendors and other organizations. In turn, that has heralded an uptick in "malicious cyber campaigns" that attack healthcare facilities, according to U.S. and U.K. law enforcement agencies.

- Security Assessments in Care Settings are intended to protect and secure health information (electronic protected health information or ePHI), from a wide range of threats, whether in emergency situations or during a system failure that constitutes a risk compromising the confidentiality, integrity, and availability of ePHI.

- During an IT audit, expert auditors evaluate your internal and external network to find out where attackers could gain access. When auditing the IT systems of a healthcare organization, auditors will also ensure that all data is being stored, and internal governance follows compliance needs associated with HIPAA, as well as any other standards that are applicable in your situation.

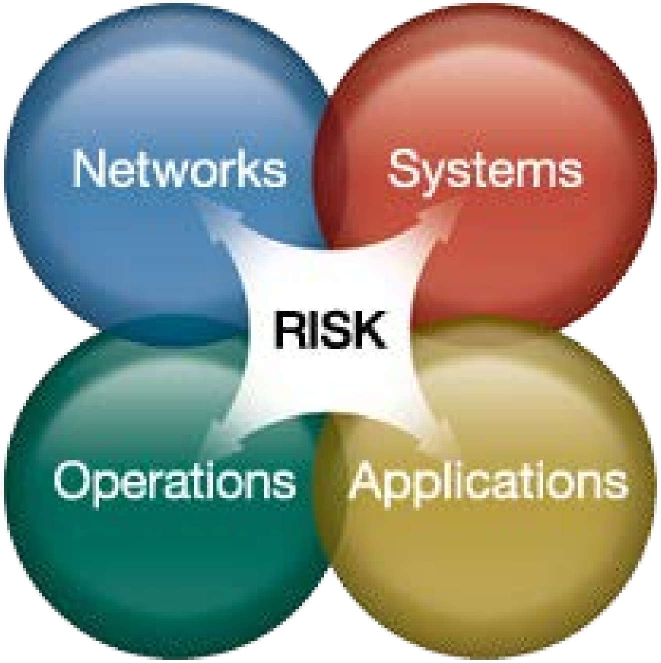
Intelligere

Information Security Assessment

- Security Risk Assessment in Care Settings are intended to protect and secure health information (electronic protected health information or ePHI) from a wide range of threats, whether in emergency situations or during a system failure that constitutes a risk compromising the confidentiality, integrity, and availability of ePHI.

- They include checks for vulnerabilities in your IT systems and business processes, as well as recommending steps to lower the risk of future attacks.

- Security assessments are also useful for keeping your systems and policies up to date



ANX

The Importance of Information Security Assessments

- **Cloud Storage:** While most major cloud providers follow standard security procedures, you still need to remain vigilant. Gartner research predicts that over the next four years, at least 95 percent of cloud security failures will be the fault of the user, not the provider. Adopting cloud visibility and control tools, such as dashboards for monitoring cloud usage, will reduce occurrences of security failures by a third.
- **Compliance**: HIPAA, FISMA, GDPR, PCI DSS -Regular internal security assessments will help to ensure you pass the third-party audits that are necessary for compliance certifications.
- **Threat Surface Increase.** Security assessments are necessary because of IoT (internet of things), virtualization, consumerization, Bring Your Own Device (BYOD), big data, and the mobile revolution.
- **Security Breach Detection.** Periodic Security assessments help organizations identify breaches more quickly. The faster you identify and contain a data breach, the lower your costs will be.

Hitachi

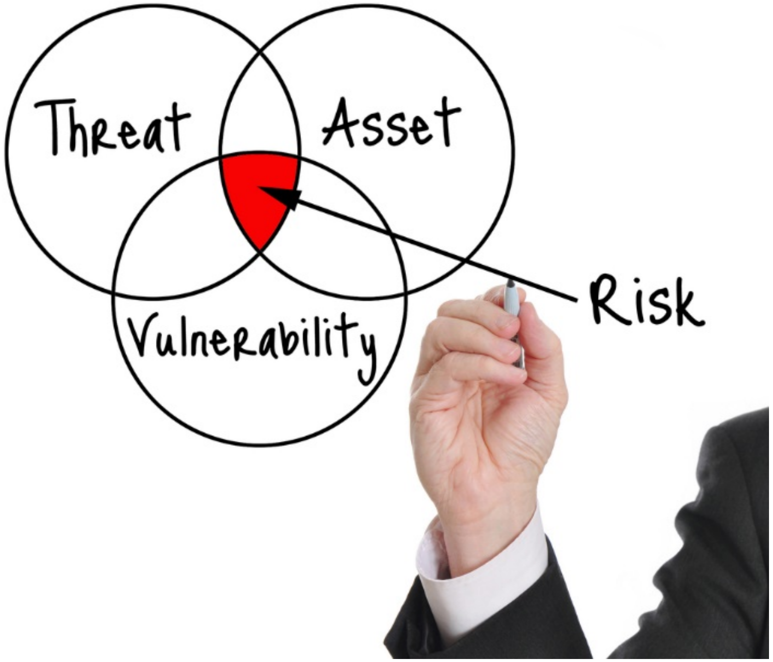
Security Assessment Steps

- **Create a core assessment team.** This core team will lead the assessment, prepare the report, and suggest recommendations.
- **Review existing security policies.** security policy should cover your security strategies, data backup plans, password management policies, security update/patch timelines, and other related details.
- **Create a database of IT assets.** Prepare a comprehensive list of all software and hardware assets that your company owns. This includes the networks, servers, desktops, laptops, software applications, websites, POS devices, the personal devices that your employees use to check emails, external drives, etc.

Threat Sketch

Security Assessment Steps cont…

- **Understand threats and vulnerabilities.** Prepare a list of all potential threats that your business could face based on past experiences, experiences of your peers, news reports, etc. Identify gaps in your system that these threats could potentially exploit.
- **Estimate the impact.** Categorize the impact of a cyberattack threat vectors as “high, “medium,” or “low” based on its severity and estimated cost.
- **Determine the likelihood.** Categorize the likelihood that each potential risk would happen as “high,” “medium,” or “low.” The risk level increases if the likelihood is high.
- **Plan the controls.** List the existing control systems in place and outline further actions that can help mitigate the identified risks. These controls can include a change in policies or procedures, application procurement, training content and configurations, or implementation of new applications and/or hardware.



Threat Sketch

Security Testing

Security testing helps you evaluate and test the security strength of your hardware, software, networks, and other IT systems.

- **Cyberattack simulation tests:** Authorized simulation attacks on your computer system help identify the weaknesses as well as the strengths of your existing system.
- **Security scanning:** Use security software to run a complete scan of applications, networks, and devices at least once a month to identify threats and risks. Most security software provides real-time and automatic scanning features.

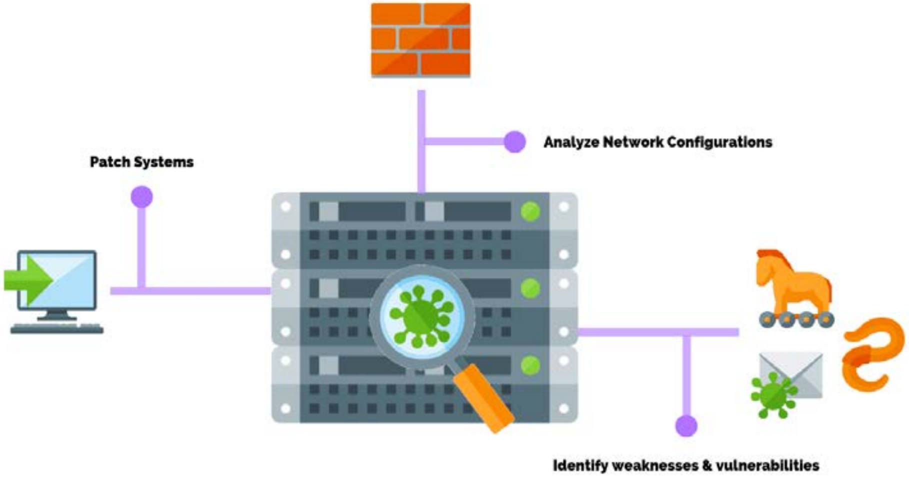
GovLoop

Security Testing cont…

- **Vulnerability scanning:** It is often difficult to spot gaps or vulnerabilities in a system that you created or that you have been using for a long time. A vulnerability assessment is a set of processes that help you identify vulnerabilities and rate them based on the severity of issue they can potentially cause. Some ways you can identify vulnerabilities include:

  - Use an Active Directory management tool to identify users with weak domain passwords. **81% of security breaches leveraged stolen or weak passwords in 2017.**

- **Ensure supplier compliance:** While you must ensure security compliance within your organization, you should also verify the credentials of your vendors and other business partners. Routinely check with your suppliers and business partners through surveys and questionnaires to ensure that they are compliant with all industry regulations.


Analyze Network Configurations
Patch Systems
Identify weaknesses & vulnerabilities

PurpleSec

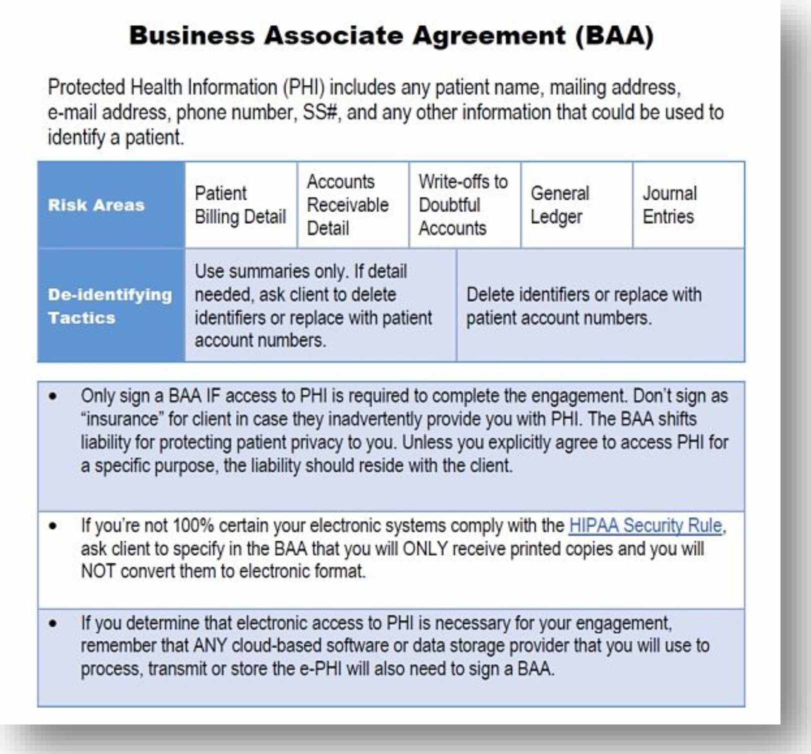
Business Associate Agreement

The Business Associate Agreement

- The agreement between a Covered Entity (CE) and a Business Associate (BA) governs the BA's creation, use, maintenance and disclosure of PHI. And it must comply with HIPAA Security, help a CE satisfy privacy rules and treat subcontractors as Business Associates.

What are Business Associates directly liable for?

- Impermissible uses and disclosures
- Failure to provide breach notification to the CE
- Failure to provide access to a copy of the ePHI to either the CE, the individual, or the individual's designee
- Failure to follow minimum necessary standards when using or disclosing
- Failure to provide an accounting of disclosures



Business Associate Agreement (BAA)

Protected Health Information (PHI) includes any patient name, mailing address, e-mail address, phone number, SS#, and any other information that could be used to identify a patient.

Risk Areas	Patient Billing Detail	Accounts Receivable Detail	Write-offs to Doubtful Accounts	General Ledger	Journal Entries
De-identifying Tactics	Use summaries only. If detail needed, ask client to delete identifiers or replace with patient account numbers.		Delete identifiers or replace with patient account numbers.		

- Only sign a BAA IF access to PHI is required to complete the engagement. Don't sign as "insurance" for client in case they inadvertently provide you with PHI. The BAA shifts liability for protecting patient privacy to you. Unless you explicitly agree to access PHI for a specific purpose, the liability should reside with the client.
- If you're not 100% certain your electronic systems comply with the HIPAA Security Rule, ask client to specify in the BAA that you will ONLY receive printed copies and you will NOT convert them to electronic format.
- If you determine that electronic access to PHI is necessary for your engagement, remember that ANY cloud-based software or data storage provider that you will use to process, transmit or store the e-PHI will also need to sign a BAA.

AICP

Penetration Testing

- Penetration tests are a vulnerability testing approach in which analysts identify potential weaknesses and attempt to exploit vulnerabilities.

- Specifically, penetration testers will first run automated scans and then manually test your website, patient portal, or other Internet-facing networks and applications to see if there is a way into your patient data using common hacker tools. If found, the testers report these vulnerabilities to you with recommendations on how to better defend the systems.

- **Rules of Engagement** Prior to the commencement of any testing, it is important to document and agree upon the conditions in which testing is to be performed and the degree of exploitation, if any, that is permitted.

- This authorizes the tester to test the environment and ensure the organization understands what to expect from the penetration test.

Xenostack

Penetration Testing cont…

- An **internal penetration test** is when penetration testers test systems (without PHI access) within your organizational network (i.e., perspective of someone inside your network).

- An **external penetration test** is when penetration testers test from a perspective of an open public network (Internet) outside of your organizational network (i.e., perspective of a hacker over the Internet).

- First, establish what your organization considers a major change. What might be a major change to a smaller organization is only a minor change in a large environment. For any organization size, if you bring in new hardware or start accepting patient data in a different way, that constitutes a major change.

BreachLock

IT Auditing

- An audit can identify gaps and expose issues with the controls in your current security systems, allowing you to address them before a cybercriminal takes advantage of the weaknesses in your systems.

- During an IT audit, expert auditors evaluate your internal and external network to find out where attackers could gain access.

- When auditing the IT systems of a healthcare organization, auditors will also ensure that all data is being stored and internal governance follows compliance needs associated with HIPAA, as well as any other standards that are applicable in the organization’s situation.

The AME Group

Security Assessment, Testing and Audit post Covid-19

- Penalties will not be imposed for noncompliance with HIPAA regulations against providers leveraging telehealth platforms that may not comply with the privacy rule during the COVID-19 pandemic will not have penalties imposed.

- Healthcare providers will be able to use any popular applications that allow for video chats, which includes Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, or Skype, to provide telehealth services without risk that OCR will impose a penalty for HIPAA noncompliance.

- **HHS Recommendation:** HHS Analyst recommend that when Pandemic normalizes Healthcare providers conduct a thorough Security Assessment to identify mitigate the new threat vectors and vulnerabilities introduced.

Help Net Security

Reference Materials

References

- Healthcare compliance and cybersecurity: Examining the needs
  - http://www.healthcarebusinesstech.com/healthcare-compliance-and-cybersecurity-examining-the-needs/
- 32% Providers Store Data in Cloud, Despite Lack of Security Resources
  - https://healthitsecurity.com/news/32-providers-store-data-in-cloud-despite-lack-of-security-resources
- Cybercriminals are 'already taking advantage' of the COVID-19 crisis
  - https://www.healthcareitnews.com/news/cyber-criminals-are-already-taking-advantage-covid-19-crisis
- Demystifying STRIDE Threat Models
  - https://dev.to/petermbenjamin/demystifying-stride-threat-models-230m
- Threat Modeling: 12 Available Methods
  - https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html
- Uncover Security Design Flaws Using The STRIDE Approach
  - https://web.archive.org/web/20070303103639/http://msdn.microsoft.com/msdnmag/issues/06/11/ThreatModeling/default.aspx
- 2015 IT Audit & Information Security Survey
  - https://ahia.org/assets/Uploads/pdfUpload/WhitePapers/AHIAITAuditAndInformationSecuritySurvey.pdf
- COVID-19 and HIPAA: Privacy, Security, and Breach Response During a Global Pandemic
  - https://www.jdsupra.com/legalnews/covid-19-and-hipaa-privacy-security-and-91596/

References

- ISACA Survey: Cybersecurity Attacks Are Rising During COVID-19, But Only Half of Organizations Say Their Security Teams Are Prepared for Them
  - https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2020/isaca-survey-cybersecurity-attacks-are-rising-during-covid-19
- 51% of Organizations Say Their Security Teams are Prepared for Rising Cyberattacks during COVID-19
  - https://www.securitymagazine.com/articles/92417-only-half-of-organizations-say-their-security-teams-are-prepared-for-rising-cyberattacks-during-covid-19
- What Does An It Audit For A Healthcare Organization Look Like?
  - https://www.valasecure.com/blog/it-audit-healthcare
- Are your vendors HIPAA compliant...are you sure?
  - https://www.imagineiti.com/hipaa-compliance/business-associates/
- Healthcare Compliance Auditing and Monitoring
  - https://emptech.com/healthcare-compliance-auditing-monitoring/
- Best Practices for Cybersecurity Compliance Audits
  - https://www.blackstratus.com/best-practices-cybersecurity-compliance-audits/
- Cybersecurity, Inside Jobs, Outside Jobs, and HIPAA
  - https://www.natlawreview.com/article/cybersecurity-inside-jobs-outside-jobs-and-hipaa
- Are Your Vendors Violating HIPAA? Why Internal HIPAA Compliance May Not Be Enough
  - https://www.beckershospitalreview.com/healthcare-information-technology/are-your-vendors-violating-hipaa-why-internal-hipaa-compliance-may-not-be-enough.html

References

- What Healthcare Needs To Know About Penetration Testing
  - http://info.securitymetrics.com/what-healthcare-needs-to-know-about-penetration-testing-lp?utm_source=blog-social&utm_medium=social&utm_campaign=social-media
- What Healthcare Should Know About HIPAA Penetration Testing
  - https://www.securitymetrics.com/blog/what-healthcare-should-know-about-hipaa-penetration-testing
- Security Risk Assessment In Health Care
  - https://resources.infosecinstitute.com/category/healthcare-information-security/security-technologies-in-healthcare/security-risk-assessment-in-healthcare/#gref
- Healthcare External Penetration Testing with Vulnerability Assessment
  - https://www.hipaatraining.net/network-assessment/
- Information Security Risk Assessment in Hospitals
  - https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5688383/
- 7 steps to pass, or better yet avoid, an OCR security audit
  - https://www.healthcareitnews.com/news/7-steps-pass-or-better-yet-avoid-ocr-security-audit
- Top IT Risks and Opportunities from an Audit Perspective
  - https://assets.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2018/P8_handout1.pdf
- Schedule a Security Audit for 2018
  - https://www.integrityky.com/schedule-a-security-audit-for-2018/

References

- Healthcare Cybersecurity In The Time Of Coronavirus
  - https://www.helpnetsecurity.com/2020/03/18/healthcare-cybersecurity-coronavirus/
- Network Penetration Testing Fundamentals
  - https://www.breachlock.com/network-penetration-testing-fundamentals/
- What is Penetration Testing? Best Tools and Techniques
  - https://www.xenonstack.com/insights/what-is-penetration-testing/
- Should You Sign a Business Associate Agreement Under HIPAA?
  - https://blog.aicpa.org/2014/09/should-you-sign-a-business-associate-agreement-under-hipaa.html#sthash.U6SfrQP4.dpbs
- 5 Free Network Security Vulnerability Scanners
  - https://www.govloop.com/community/blog/5-free-network-security-vulnerability-scanners/
- 3 Types Of Cybersecurity Assessments
  - https://threatsketch.com/3-types-cyber-security-assessments/
- How Often Should You Perform A Network Vulnerability Scan?
  - https://purplesec.us/how-often-perform-vulnerability-scan/
- How Does an IT Audit Differ From a Security Assessment?
  - https://www.dnsstuff.com/it-security-audit-vs-security-assessment
- Healthcare cloud security: Staying current with BAAs, SLAs
  - https://healthitsecurity.com/news/healthcare-cloud-security-staying-current-with-baas-slas

Questions

Questions

Upcoming Briefs

- Maze Ransomware
- Recent Advertisements of Medical Databases on Cybercriminal Forums

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity
Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV