children's
MEDICAL CENTER

Session 2.02: Achieving an Adequate Level of Security Without Hindering Patient Care

Jody S. Hawkins, ISO

Dallas, Texas

Overview

“Key Points” Preface

Measuring Security Levels

Balancing Security and Patient Care

Learning Curves for New Implementations

Utilizing an Entire Security Architecture

Conclusion

Key Points

This presentation does not take any cost analysis vs. risk acceptance into consideration

There will always be an acceptable level of risk, but this presentation works under the assumption that those processes have been completed and an acceptable solution is available

Measuring Security Levels

Very difficult to measure and prove

- Subjective – relying on Security Expert
- Objective – need (sometimes) years of data

Risk Analysis and Gap Analysis a must

Every organization will be different but some suggestions would be:

- Network Vulnerability, Virus Activity, Password Management, Perimeter Defense, User Education, Account Management, etc. Create an overall Security Health Score
- Example – 10 measurable security facets with an overall health score of 100
  - Each facet has individual weight of 10 with a cumulative max of 100, but not necessarily a minimum of 0
- Negative scoring would include items like Network Vulnerabilities and Virus Activity

Measuring… continued

Formulas (MS Excel is an excellent tool)

- Example of Negative Scoring
  - Low, Medium, High - .001, .01, and .1 respectively
  - Take a sum of those values and multiply by 10 (highest possible score and conversion of decimal point) and then subtract that value from 10 and post the difference as the score.
    - If you have 0 vulnerabilities you have a Security score of 10. With 1 low and no medum or high you have a 9.99
    - 10 high, 3 medium and 10 low produces a score of -0.4
- Negative scoring makes perfect since if you look at the big picture
  - All aspects of security are perfect except one (giving you a Security Health Score of 90), but you have 50 high network security vulnerabilities which would produce a score of -40, thus bringing down the overall score to 50 (or 50% out of 100%)
- This can be used on all “low, med, high” outputs

Measuring… continued

Formulas

- Audit vs. Breach – variables are # of audits performed and #of breaches found.
  - Takes into consideration the number of audits performed when weighting the number of breaches (i.e. 10 audits with 1 breach produces a lower score than 100 audits with 1 breach)
    - (((# of audits * 10)+(# of breaches * 10))/ # of audits)10=Score
- Security Investigations – variables are total # of investigations, # of formal investigations (formula can automatically figure preliminary inquiries), # of investigations dealing with PHI, and finally the number of investigations that found malicious intent by a user
  - (((# formal * 0.5)+(# PHI * 1)+(# Malicious * 1.5))/ # investigations)10 = X then 10 – X = Score

Measuring… continued

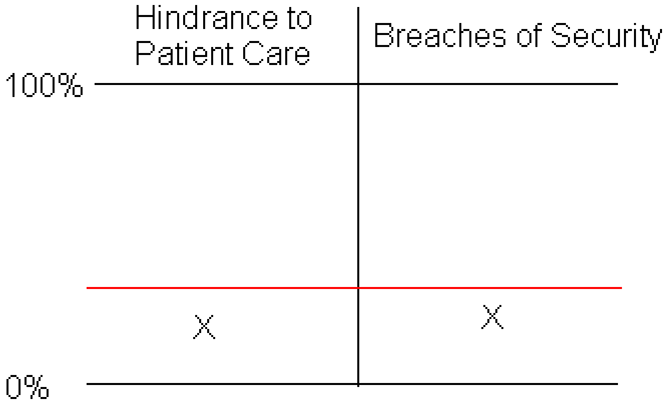
Sum it all up

- Give all facets identified an initial measurement of 0 and keep a 0 for all facets that you currently do not have a means to measure (i.e. you need a network vulnerability assessment tool to perform audits and produce scores)
- Define acceptable percentages based on findings and best business practices
- I have defined my scoring process as:
  - Green – 80% - 100% - Very unlikely an attack will be successful or a breach will occur
  - Blue – 68% - 79% - Not likely an attack will be successful or a breach will occur
  - Orange – 46% - 67% - Somewhat likely an attack will be successful and/or a breach will occur
  - Red – 25% - 45% - Very likely an attack will be successful and or a breach will occur
  - Black – 0% - 24% - Extremely likely an attack will be successful and or a breach will occur

Balancing Security and Patient Care

An Uneven Scale

- 0 breaches of Security does not equal 100% hindrance to Patient Care
- Red line is an arbitrary mark representing a break point. If the mark is hit the process needs change



Balancing… continued

Note – the right side of the chart "Breaches of Security" is likely or probable breaches.

Defining Hindrances

- Is 16 seconds a hindrance to patient care?
- What about 32 seconds?
- How about 10 minutes?
- A good deal of security is user education

Learning curves

- New implementations need time for the users to become proficient.
  - Will have slightly higher hindrances at first, but will drop as the users become accustomed to the new procedures

Balancing… continued

Calculating hindrances

- Can be accomplished in many ways
- Walk the floors and ask them what they think
  - Questionnaires and Surveys
- Always involve leadership of affected departments
  - Show audit, questionnaire and survey results and let them have buy-in to the process.
  - Support from top down is critical

Calculating the learning curve

- Variables
  - How does the new implementation affect the end users?
    - New login method?
    - Requiring stronger passwords?
    - Look and feel of application changed?
    - Additional end-user responsibility requirements?
  - How does the new implementation affect other applications currently in use?

Balancing… continued

Calculating the learning curve

- Implementation of stronger password policy
  - User involvement is HIGH
  - User difficulty in learning new process is LOW
    - The user already understands the use of passwords
  - Lower initial impact by leading the implementation with proper user education
- Through input collected from end users you can closely predict initial impact
- As users become accustomed to the change the hindrance should be little to none after the initial first weeks
- If the users are going to be forced to change password the hindrance will go back up at force change time
- This type of effort could take a year or more to level out

Utilizing An Entire Security Architecture

Linking it all together

- A solid security architecture designs itself once all the above is accomplished
- List all measurable aspects (including hindrances)
  - You will see your deficiencies and strengths
  - Becomes a living gap analysis
- Example
  - scenario where lack of training for password management has caused the overall security score to drop. With all other individual aspects being at adequate levels, look at the chart to the right of the formulas at lines 5 and 11. You should see that lines 5 and 11 are considerably lower than all other scores and are associated with Failed Logon Attempts and Security Investigations, respectively

Utilizing… continued

In this scenario we can use an example of a new password management policy implementation where proper education did not get to the end users, causing a drop in the overall security score

  - In this example, 150 logon attempts were audited and showed that 6 accounts were locked, 8 went over 6 attempts and 27 had minor trouble logging in

- Coupled with Security Investigations, the score drops even more dramatically due to the fact that users will be sharing passwords, using each others logons, leaving workstations logged into clinical applications, and writing their passwords down and leaving them next to workstations

Utilizing… continued

Breaches will occur due to the fact that the patient care providers will be focused on their primary job responsibility… the delivery of patient care

- If security inhibits the delivery of patient care to the point of breakage then security will be breached
- In this scenario, you can see how easy it is to notice an area that needs improvement and you can make sound decisions based on facts that will fix security problems before major breaches occur

Risk Assessment and Gap Analysis is a must, but most focus on the security "holes" that are found

- Learn to look at Security as a "whole" and the "holes" will be obvious

Conclusion

Keeping thorough and concise documentation is a must

- Over time, this documentation can be utilized to produce objective information that can be used to continually tweak the overall security architecture for a specific organization

There are no tools available

- Tools are good for individual aspects
- This is the job of the Security Professional

Take control of the Security Architecture in your organization

- Will give you a much better picture of security
- Will give the confidence to you
- Will give confidence to affected departments and users
- Will gain more support for security implementations