DueNorth
SECURE HEALTHCARE

How to Understand Information Security Risk For the Non-IT Professional

1

DueNorth
SECURE HEALTHCARE

Your Presenters

Ken Satkunam, CISA, CISM
Principal Consultant
DueNorth Security, LLC

- 25 years of information technology experience
- Has held positions from support desk to CIO

Deanna Allen, BHA, RHIA, CHC, CHPC
Compliance, Privacy and Security Officer, HIM Director
Ivinson Memorial Hospital

- 33 years of healthcare experience
- Compliance, Revenue Cycle, and Health information Management on both small and large healthcare organizations

Mark Schlader, HCISPP
Principal Partner
DueNorth Security, LLC

- 6 years of information security experience
- 25 years of sales now used to sell security to healthcare facilities that need it!

2

MS1

DueNorth SECURE HEALTHCARE

How to Understand Information Security Risk for the Non-IT Professional

Objectives:

- Better understand how to prioritize information security risks that have been identified through a risk analysis
- Learn how to work cohesively with IT to develop a risk management plan that everyone can understand, accept, and realistically accomplish
- Learn how to more effectively communicate information security risk and security rule compliance to executive management and board members

3

MS1

DueNorth SECURE HEALTHCARE

Poll #1

Who do you work for

A. Larger covered entity – 500 plus employees
B. Small covered entity – less than 500 employees
C. Business Associate
D. Independent Consultant/Attorney

4

MS1

DueNorth SECURE HEALTHCARE

Poll #2

How Involved are you with managing your organization's information security program

A. Very Involved
B. Somewhat Involved
C. Not Involved
D. We don't have an information security program

5

DueNorth SECURE HEALTHCARE

Step #1 - Get Everyone Speaking the Same Language

Definitions

Risk Analysis - an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health **information** held by the covered entity.

Information security - managing the risk to the confidentiality, integrity, and availability of information using administrative, physical, and technical controls

Risk – the likelihood that a threat will expose a vulnerability to have an adverse impact on an asset

Vulnerability - a weakness which can be exploited by a threat.

Threat – physical, insider, cyber, and more. Always changing.

6

Security and Compliance

It is impossible to prove HIPAA Security rule compliance without a formal information security program

So, Who's Job is it?..... EVERYONE'S

Benefits to approaching enterprise-wide security 1st, HIPAA Security Rule compliance 2nd

1. It is easier to enforce the same set of policies and procedures across the entire workforce
2. Protect all your information, not just ePHI
3. Build a culture of security, gain buy-in
4. Create a more impactful case for budget and resources

7

Step #2 - Get The Right People at the Table

Information Security is a Corporate Culture Issue

Who needs to be involved? – IT, Compliance, Executive Management, the Board

Simplify the Risk Analysis – Complexity is the enemy of Information Security

How to get people engaged?
1. Have a breach?
2. Get Ransomware
3. Talk less about compliance and more about money and patient care – Show an ROI

Who writes information security policies? Who sets information security budget?

8

Developing a Risk Management Program

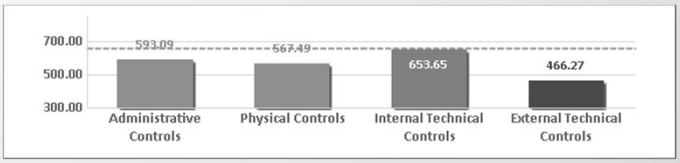
1. Select a Team
2. Develop a reporting structure to the Top
3. Create a Plan: Document your Process, Findings and Actions
4. Perform a Security Risk Analysis
5. Create a Budget
6. Develop an Action Plan

9

Step #3 – Quantitative and thorough Risk Analysis

Search for Simplicity

- The more objective the better – yes/no questions
- Quantitative results – you cant manage what you cant measure

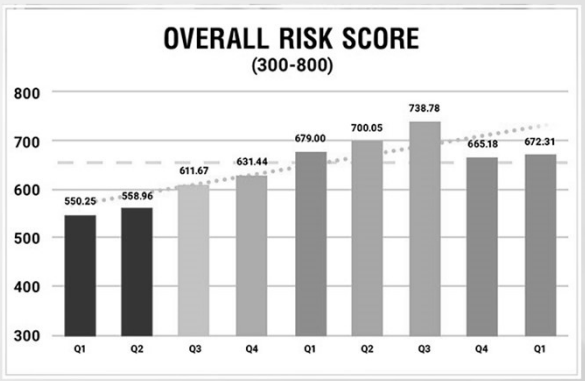


10

Step #4 – Manageable Remediation Plan

Be Able to Reward Success!

- Rank and Prioritize Risk
- Set Budget and Resources
- Set yourself up for success and ask that everyone is held accountable



11

Step #5 – Get Third-Party Validation

- Expert advice on the front-end can save thousands spent on security products and services
- More justification when requesting changes to policy and procedure or requesting budget
- Serves as a mediator between departments

12

DueNorth SECURE HEALTHCARE

Recap

Step #1 - Get Everyone Speaking the Same Language
Step #2 - Get The Right People at the Table
Step #3 – Quantitative and thorough Risk Assessment
Step #4 – Manageable Remediation Plan
Step #5 – Get Third-Party Validation

13

DueNorth SECURE HEALTHCARE

Q and A

14