Relational Security Corporation

"Making your HIPAA Security Efforts Last"

Round One is coming to a close

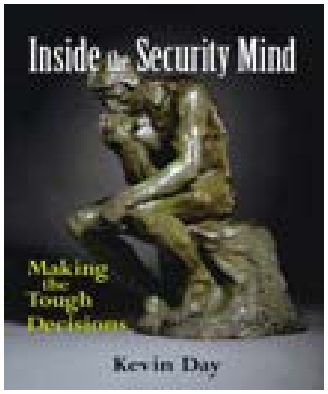
But the Fun is far from over!

Kevin C. Day

CTO

Relational Security Corporation

www.RSAM.net

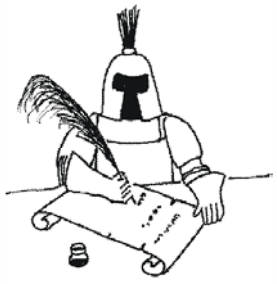


Make your Efforts Stand the Test of Time

- Many organizations have not had the time & resources to do a thorough job
- Most likely the direction & approach changed several times throughout the process.
- While focusing so much on getting to D-Day, have they acquired processes and tools that will maintain the compliance?
- Time to take a look and see what we have

You Can't Maintain Compliance if…

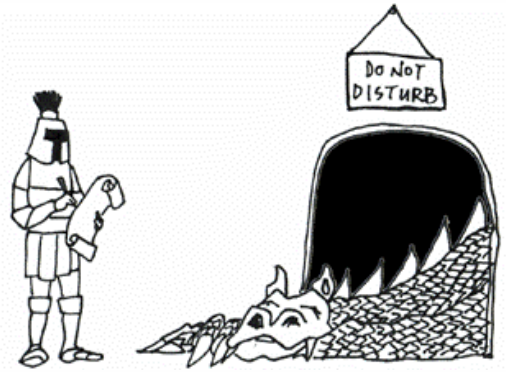
1. Your HIPAA budget is drastically cut after D-Day!
2. There is no formal process to review & update your policies & procedures
3. You don't continually validate that the policies are being followed
4. You can't continually & consistently update your Risk Assessment (not "annual" but "continual")
5. You don't have a Risk Inventory (where is the ePHI?) to enforce your standards and monitor compliance
6. You have not incorporated Change Management processes that ensure changes to the environment follow the standards



Reviewing the Risk Assessment

Your Risk Assessment will continue to be the key to Compliance.

- If one day you look and realize your risk assessment is no longer accurate… you are no longer HIPAA Compliant!



- Was it is truly thorough?
  - Did we get enough details?
  - Were the results actionable?
  - Did we rush to meet the deadline?

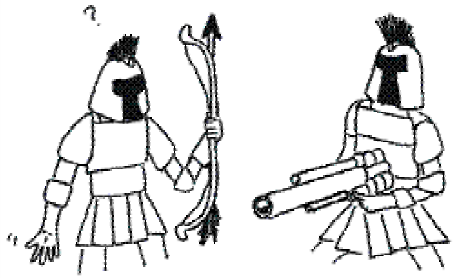
- Are processes and tools in place to:
  - Review it?
  - Update it (newly acquired assets & changes to existing assets)?
  - Make continual use of the results?

- Will it withstand investigation?

Make your Processes and Tools Last

HIPAA will not be the end of the saga…..

- Sarbanes Oxley or its equivalent will soon apply to everyone.
- Make sure your existing work & tools can expand beyond “HIPAA”.



Don't Think your Done!

Continue to Expand your efforts

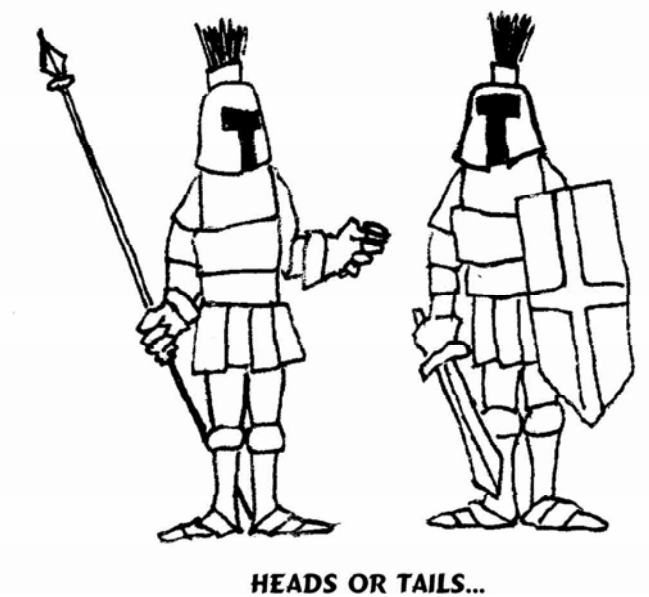
- What was considered as the basis for "reasonable control" in Year 1 will certainly not be reasonable in Years 2, 3 & 4.
- After major risks are addressed, other risks which were once "unreasonable" will now be within reach
- You must continually expand your assessment and standards to include stronger controls
- In 2006 you can't just review the 2005 documents and say "everything is the same… so we are done"

Learning from Other Industries

Common Pain-Points we hear from the financial industry (GLBA)

- We thought the regulations were broad enough to take a high-level approach…. when we were finally audited the inspectors demanded details
  - How can you secure data if you don't even know where it resides?
  - How can you security your applications if you don't even have a detailed list of their controls
- Three years ago we spent a great deal of time and effort in our compliance efforts. Now that we are actually being audited I find most of my data is 3 years old!

Will I be compliant next year?



HEADS OR TAILS...

Thank You

Contact Information:
Kevin C. Day

kday@relsec.com
www.RSAM.net