Challenges to Implementation of [real] Information Security

August 21, 2002

Chris Apgar, CISSP
Kate Borten, CISSP
Ken Patterson, CISSP

Chris Apgar, CISSP

- Former state regulator turned private sector HIPAA "expert"
- Security & HIPAA compliance officer for Providence Health Plan, a moderate sized regional health plan that is part of large delivery system
- "Volunteered" for HIPAA & security while managing Y2K remediation

Chris Apgar, CISSP (cont'd)

- Chair, Oregon HIPAA Forum Transaction & Code Set Subcommittee
- Past Chair, Oregon Medicaid contractors HIPAA task force
- Advisory board member, *HIPAA Compliance Insider*
- Past board member, Privacy Officers Association

My Favorite Soap Box

- The “Rodney Dangerfield complex” or “I get no respect”
- Security & privacy deemed important challenges but limited resources available to address
- Difficult to develop ROI for security – cost avoidance versus a profit making venture
- Overcoming the belief, “it won’t happen to me”

Senior Management Education (or lack thereof)

- The business of keeping the doors open versus attending to the details
- Overcoming the belief that security is another IT initiative
- No final security rule hampers efforts to acquire resources
- Problem generally not getting to the top but keeping top management engaged

Solutions & Suggestions

- Tie security to ROI – what is the competition doing, positive PR, etc.
- Remind Privacy Rule & statute mandate sound security practices
- Educate, educate, educate
- Use horror stories judiciously

Solutions & Suggestions

- Present options, accept risk and remain flexible
- Remember brevity with top executives – make your point quickly and avoid fluff
- Cultivate security advocates within and outside the organization
- Incorporate a bottom up approach (I.e., train end users, period security announcements to staff, etc.)

Solutions & Suggestions

- Focus on culture, business process versus technology – change the belief "this is only an IT issue"
- Partner with regulatory, compliance, clinical – generally deep concern felt for privacy of patient/member
- Patience & a sense of humor a must!

Kate Borten, CISSP

- In healthcare IT for over 20 years … designing & implementing IT solutions for clinical and business functions (at Harvard U. affiliates)
- Got "stuck" with starting up first-time comprehensive information security program at Mass. General Hospital (IDS) in the early 1990s … found out there's a lot more to it than passwords!

Kate Borten, CISSP (cont'd)

- Chief Information Security Officer, CareGroup
  - Set up corporate-wide comprehensive infosec program
- Now, President, The Marblehead Group, Inc.
  - National healthcare privacy & security consulting

A Few of the Numerous Challenges

- Understanding
  - Lack of health industry knowledge of the field
- Importance
  - InfoSec plays second fiddle to privacy - yet breaches & lawsuits usually due to infosec flaws
- Scope
  - Due diligence => protection of *all* information assets, not just HIPAA stuff
- Technology
  - Big problems remain unsolved

Culture Change

- One of the biggest challenges: changing ***people***
- Need to understand and work to modify ***attitudes & behavior***

Culture Change Needed! Real Examples

Security principle: Passwords must be hard to guess & kept secret

- Clinton signs the e-sign bill using password "Buddy," a radiologist picks password "RAD"
- Passwords stuck on computer screens, under mouse pads, on keyboards, on stethoscopes
- Boss says, "Tell me your password 'cause I don't have time to submit the form and go through training to get my own."

Culture Change Needed! Real Examples

Security principle: Everyone is personally responsible for ensuring good security through their own behavior and through reporting incidents

- "The computer people handle that [*i.e., it's not my job*]."
- " I'm not gonna rat on my friend! [*and what's the big deal about looking up his girlfriend's lab test results anyway*?]"

Culture Change Needed! Real Examples

Security principle: Avoid confidential conversations where they can be overheard

- "We've asked him to lower his voice when he's discussing patients in the ER, but I guess he just has a naturally loud voice."
- "We're so busy that we need to catch up on cases whenever we bump into each other [*such as in the elevator, walking down the hall, in the cafeteria*]."

Culture Change Needed! Real Examples

Security principle: Destroy media (shred paper, chip disks, etc.) containing confidential data when no longer needed

- "But it's only a phone message slip with the patient's name and number on it."
- "But it's just a floppy disk and I'm using it at home now for other files."

Good News

- Little/no technology required
- Hence, relatively low budget
- Most “bang for the buck” - can get great results through strong workforce education programs
- And it can be fun!

Ken Patterson, CISSP

- Information Security Officer for Harvard Pilgrim Health Care

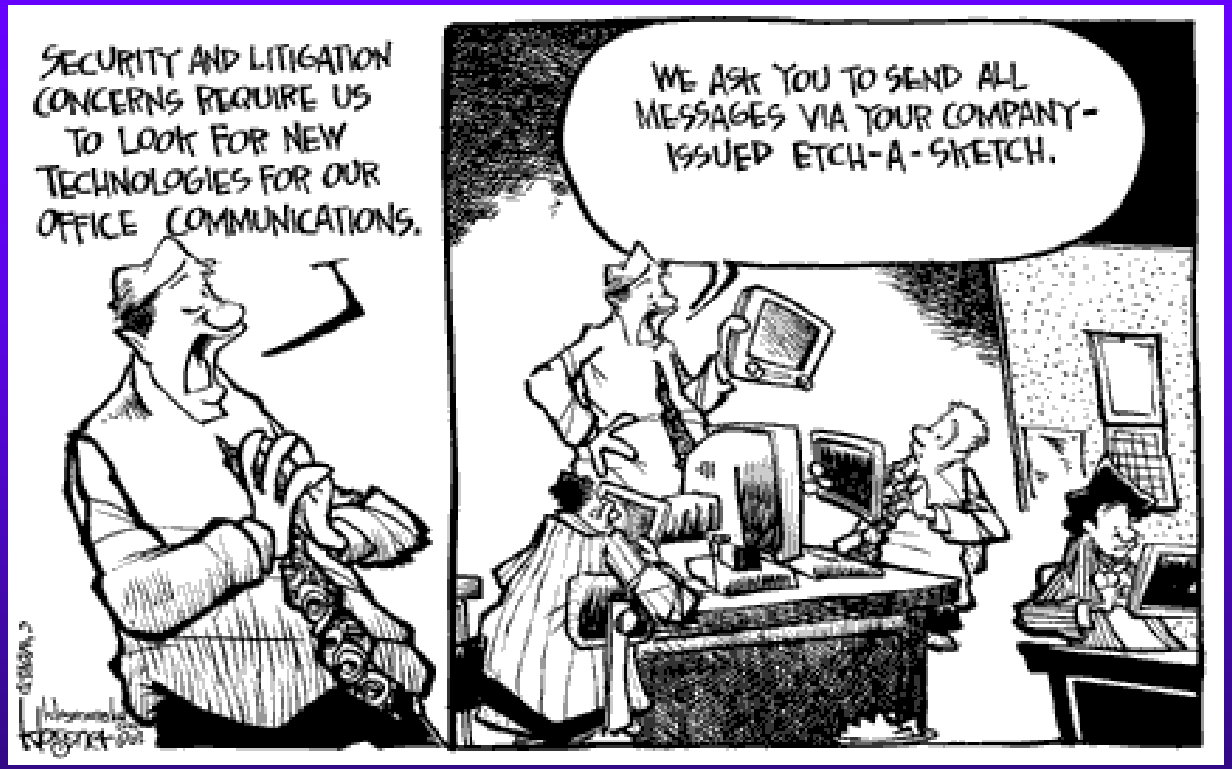
"This **is** the hot young security officer"

copyright 2002 john klossner, www.jklossner.com

Technology Challenges

- Technical security mechanisms
  - Processes that are put in place to guard against unauthorized access to health information that is transmitted over a communications network
  - When using open networks, some form of encryption should be used
  - Small provider example: encryption must be used to transmit or receive health information when the provider chooses to use the Internet

Technology Challenges: Secure Messaging / E-mail



copyright 2002 john klossner, www.jklossner.com

Secure E-mail Solutions

- Client based solutions: client software implemented as a “plug-in” or “add-on”.
- Pros: client to client security
  - Protects message from internal staff
  - Integrated into existing email environment
- Cons: Requires end-user training, including installation at the client level
  - End user responsible for e-mail security
  - Very difficult to centrally scan for viruses, perform content checking, and message archiving

Secure E-mail Solutions (cont.)

- Web based solutions: web interface where messages are checked, signed and encrypted at the web server – can be outsourced
- Pros: No installation at client or local network
  - Low initial cost and administrative overhead
  - Can provide extensive message tracking
  - Any browser can easily access
- Cons: A new and separate e-mail system
  - Dependency on supplier
  - Not always fully secure

Secure E-mail Solutions (cont.)

- Server based solutions: adds a centrally controlled layer of security to the existing mail server
- Pros: uses existing e-mail environment, so no client installation, low level of user training required
  - Centrally control and maintain e-mail policy
- Cons: internal security issue still present
  - Client to client not 100% secure
  - Resources for administration and central control are required

No Free Lunch

copyright 2002 john klossner, www.jklossner.com