

Implementing Security in an Academic Medical Center

Presented by

Larry Lotenero, CIO

Jose Claudio, Security Officer

Binh Nguyen, Security Manager

Agenda

- ***UCSF Medical Center Overview***
- ***Initial Approach***
- ***New Approach***
- ***Results***
- ***Next Steps***
- ***Conclusion***
- ***Q&A***

UCSF Medical Center Overview

UCSF Medical Center and UCSF Children's Hospital are recognized throughout the world as leaders in health care, known for innovative medicine, advanced technology and compassionate care. As an academic medical center, we offer pioneering treatments not widely available elsewhere. For example, we have the only nationally designated Comprehensive Cancer Center in Northern California.

UCSF Medical Center Overview

- 2 hospitals, 5 business offices, 5 remote clinics, and outpatient facilities
- 688 beds
- Metropolitan Area network is provided via a fully meshed GigE network
- 7600+ nodes
- 220+ servers
- 6 firewalls
- 2 redundant 6 Gigabit links to the Internet

UCSF Medical Center Overview

As a result of the UCSF Medical Center and Stanford Medical Center de-merger, UCSF medical center was forced to create and implement a security plan. The first step taken was to create a four year security plan which covered:

- Password security
- Secure remote access
- Border firewalls at Internet connections and between the Medical Center and Campus networks
- Intrusion Detection
- Access Control
- Security Policies

Initial Approach

- Write the security plan
- Communicate and Implement solutions in the security plan
- Write policies
- Communicate and implement policies
- Move on to other projects

Initial Approach

Unfortunately this approach was not very successful

- Few understood the need for security
- Medical Center and Campus interdependencies surfaced
- Medical Center, Campus, and global research collaboration became an issue
- The smooth road to security, created in the security plan and policies became rocky

New Approach

- Asked and received executive level support
- Formed a committee of Medical Center and Campus representatives
- Changed communication approach to include department support staff, managers, and executives
- Changed implementation plan from all at once security to phased security
- Used audits, government regulation, and news of security breaches to communicate the need for security

New Approach

Executive management support was instrumental to the success of the project

- They re-enforced the project teams message that security protected everyone and made business sense
- When escalated to they supported the project team and did not back down to political pressures
- Security was often discussed at executive staff and management meetings
- Funded the security initiatives

New Approach

Having a committee of Medical Center and Campus representatives actively participating in meetings and guiding the process was another key to success

- It established two way communication between the client departments and the security team
- Their feedback helped guide the security team
- Their involvement helped support the security initiatives to their respective clients
- Being part of the team gave them ownership of the outcome

New Approach

Targeted communications to support staff, managers, and executive staff helped raise the awareness of the project and the effect each implementation phase would have on their work life

- Taking advantage of monthly meetings with the campus computer support staff to communicate the plans, allowed them to ask questions and feel comfortable with the changes
- Presenting at several Medical Center management meetings helped the managers understand the plan and also gave the executives an opportunity to voice their support
- Presenting to the executives in groups or in one on one sessions helped them understand the plan, which translated into informed support

New Approach

Changing the implementation plan to a phased approach, made the changes easier to accept and established credibility

- It helped the security team focus on one change at a time
- The success of each change established credibility with the clients, support staff, and management team
- Subsequent successes made the road to success smoother by making changes an after thought in everyone's minds

New Approach

Audits, government regulation, and news of security breaches were used when it made sense to reinforce the need for security and the consequences of not having good security practices in place.

- These tools were used to inform not threaten
- Used when appropriate

Results

Then :

- Weak passwords and lack of enforcement was the norm

Now:

- Strong passwords are enforced on Wintel systems
- Password on legacy systems are enforced based on capabilities

Results

Then :

- Network opened to the world

Now:

- Cisco Pix 535 firewalls used at Internet and Campus network borders
- Full restrictions enforced on Internet
- Restrictions between Campus and Medical Center network permit collaboration
- Cisco Secure Policy Manager used to manage Pix firewalls

Results

Then :

- No intrusion detection systems or network monitoring systems

Now:

- Cisco Net Ranger Intrusion Detection Systems implemented
- Cisco VPN/Secure Management Solution used to manage IDS
- Tripwire for system file protection on servers
- Cisco Enterccept and Cisco Secure Agent for host based IDS/IPS
- CiscoWorks, HP Openview, SolarWinds, NetScout, and InterMapper used to monitor network

Results

Then :

- No secure remote access

Now:

- 3 Cisco 3060 VPN concentrators in use for secure network access
- Cisco SSL Hardware Content Switching for secure web access
- SSL for secure web access
- Secure Telnet Gateway

Results

Then :

- OC3 155 megabit ATM Sonet Ring
- Single 100 megabit link to Campus network
- 100 megabit Internet connection

Now:

- Fully meshed 1 Gigabit Metropolitan Area Network
- 4 one gigabit connections to Campus network
- 4 one gigabit connections to Internet
- Full Infrastructure upgrade at CORE and distribution network

Results

Then :

- Stagnate anti-virus process

Now:

- Active anti-virus management
- Regular scheduled updates and scans on desktops
- Active scans and virus detection/prevention on e-mail gateways
- Scanning network for vulnerabilities
- Customer awareness has been heightened

Results

Then :

- Manual patch updates to desktops

Now:

- Remote push using SMS
- Installation via login scripts when necessary

Results

Then :

- Very few security policies

Now:

- Master Information Security Policy developed, approved, and posted
- Multiple procedures supporting Master Information Security Policy have been developed

Results

Then :

- No security plan

Now:

- 4 year security plan written and approved
- Security plan is reviewed and updated yearly

Results

Then :

- No network architecture and security team

Now:

- Network architecture and security team in place

Next Steps

- Rolling out secure e-mail – Tumbleweed
- Implementing secure zoning within data center
- Piloting single sign-on
- Testing 802.1x network port security
- Conducting HIPAA security risk assessments

Conclusion

- Change is not easy, but having management support helps make it happen
- Key stakeholders need to feel they have a say in the changes being made, their participation creates ownership
- Flexibility leads to success
- Communicate often
- Have a plan and be ready to implement it
- Maintain an open mind

Thank you for your attention!

Questions?

Contact Information

Larry.Lotenero@ucsfmedctr.org

Jose.Claudio@ucsfmedctr.org

Binh.Nguyen@ucsfmedctr.org