NCHICA

Transforming Healthcare from Volume to Value

What is a 'Culture of Security' and *Where Can I Get One?*

James C. Murphy

GSEC, CISSP-ISSMP, CISA, CISM

Information Security Consultant

jcm0011@earthlink.net

How we got here!

"As the role of information grows beyond anyone's reckoning, it grows to be too much. "TMI" people now say. We have information fatigue, anxiety, and glut. We have met the Devil of Information Overload and his impish underlings, the computer virus, the busy signal, the dead link, and the PowerPoint Presentation."

James Gleick, 2011.
The Information: a history, a theory, a flood.
Vintage Books/Random House, Inc. New York.

This Presentation is…

Not about personal security –

Major commercial organizations

Credit cards,

ID theft,

Is about organizational information security

Servers,

Networks

Desktops

specifically within healthcare

A 'Culture of Security'

Creating a culture of security – ISACA
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Creating-a-Culture-of-Security.aspx

Installing a culture of cyber security
http://www.net-security.org/article.php?id=2304

How to build a culture of security
http://www.itsecurity.com/features/culture-of-security-071607/

Company name!
http://www.cultureofsecurity.org/

Cisco
http://www.cisco.com/web/about/security/cspo/docs/creating_culture_of_security.pdf

A 'Culture of Security'

So, what do we mean about this??

For a better understanding:

What is the Counter
– antithesis –
of a Culture of Security?

How about the 'Culture of the Attacker'?

What is a
'Hacker'
'Cracker'
'Attacker'?

A 'Culture of the Attacker'

"Hackers are part of a subculture that is constantly in flux, making it very resistant to mainstream culture. …The Hacker subculture is a strong entity that will remain so due to its constant flux and increasing collaboration of knowledge."

https://sincdav.wordpress.com/2012/02/10/hacker-as-subculture/

A 'Culture of the Attacker'

Is there a Hacker Ethic for 90s Hackers?

by Steven Mizrach

http://www2.fiu.edu/~mizrachs/hackethic.html

1. Hackers (Crackers, system intruders)
2. Phreaks (Phone Phreakers, Blue Boxers)
3. Virus writers (also, creators of Trojans, worms, logic bombs)
4. Pirates [Breaking, stealing code]
5. Cypherpunks (cryptoanarchists)
6. Anarchists [distributing illegally obtained information]
7. Cyberpunk [all the above]

Asymmetric Warfare

All participants have *much* more knowledge of networks and servers than you or I!!

- High intelligence
- *Superior* tech/network knowledge
- Well connected community
- Frustrated with current position
- Seeking better job/income
- *No scruples!!*

A 'Culture of the Attacker'

Three divisions of attackers

1. Hackers themselves
   - In it for the money
   - "Nothing personal"
2. Middle level
   - Hacker recruiters
   - Providing tools, dispensing pay
   - Could be multiple middle levels
3. Back end
   - Organized Crime?
   - Governments?
   - International reach.

Check out Infragard – FBI Infosec liaison

A 'Culture of Security'

A 'Culture of Security' is the counter to the 'Culture of the Attacker'.

Why is this so important??
I have a firewall and Policies!!

Nothing has happened to my organization…

YET!!!

Mobile Device Management:
Context – *here's why!*

Why Hackers Are Targeting Health Data

By Marianne Kolbasuk McGee, July 7, 2014.

http://www.healthcareinfosecurity.com/hackers-are-targeting-health-data-a-7024/op-1

"While a stolen Social Security number might sell for 25 cents in the underground market, and a credit card number might fetch $1, "A comprehensive medical record for me to get free surgery might be $1,000,""

John Halamka, CIO, Beth Israel Deaconess Medical Center, Boston.

A 'Culture of Security'

and…

"By 2017, the global Cyber Security market is expected to skyrocket to $120.1 billion from $63.7 billion in 2011"

http://www.go-gulf.com/blog/cyber-crime/

Viruses, malware, worms, trojans	50%
Criminal insider	33%
Theft of data-bearing devices	28%
SQL Injection	28%
Phishing	22%
Web-based attacks	15%
Social engineering	17%
Other	11%

A 'Culture of Security'

"By 2017, the global Cyber Security market is expected to skyrocket 50 $120.1 billion from $63.7 billion in 2011"

http://www.go-gulf.com/blog/cyber-crime/

Data Breach by Industry:	
Medical, Health Care	*38.9%*
Business	35.1%
Educational	10.7%
Government, Military	9.9%
Banking, Credit, Financial	5.3%

A 'Culture of Security'

and this…

Major medical records breaches pass 1,000 milestone as enforcement ramps up

Joseph Conn, June 13, 2014, Modern Healthcare

http://www.modernhealthcare.com/article/20140613/BLOG/306139996?AllowView=VDl3UXk1Ty9DL2VCa0IvREE0M3hlMFdvakVVZEErQT0=&utm_source=link-20140613-BLOG-306139996&utm_medium=email&utm_campaign=hits&utm_source=link-20140613-BLOG-306139996&utm_medium=email&utm_campaign=hits&utm_name=bottom#

A 'Culture of Security'

not to mention…

Lawsuits permitted for organizational breaches!!

FEDERAL TRADE COMMISSION v. WYNDHAM WORLDWIDE CORPORATION - August 24, 2015

"The court determined that lack of adequate security provided by Wyndham is, in fact, engaging in "unfair or deceptive acts or practices in or affecting commerce" – the very thing the FTC is designed to prevent."

http://brilliancesecuritymagazine.com/cybersecurity/court-rules-the-government-can-punish-cyber-attack-victims/

A 'Culture of Security'

one suggestion:

Disconnect servers from the internet
Air-gapping the servers!

Researchers hack air gapped computer using a simple cell phone.

Kim Zetter Wired, Security 07.27.15.
http://www.wired.com/2015/07/researchers-hack-air-gapped-computer-simple-cell-phone

A 'Culture of Security'

Building the C.O.S.:

Tone At The Top…*and* down to the end of the hallway!

- Ramp up IT tech support staff (not easy!)
- Data protection (networks, desktop devices, servers – Disaster Recovery)
- Logging (networks and system/application access)
- Mobile Data Management/Data Loss Management (Multiple vendor solutions)
- Audit Preparation and Response
  - What you say you are doing
  - Are you doing what you say?
- Awareness *and Responsibility* training

Assistance Needed!

External Service Vendors (Acronyms):

- Managed Service Providers (MSP)
- Managed Security Services Providers (MSSP)
- Intrusion Prevention/Detection System (IPS/IDS)
- Security Information & Event Management (SIEM)
- Data Loss Prevention (DLP)
- Mobile Data Management (MDM)
- Endpoint Protection (EP)
- Business Service Management (BSM)
- Log/Threat/Vulnerability/Compliance Management

Outsourcing Security?

Server/storage service organizations
The 'Cloud!'

Data protection

Data management software

Access control

Network transmission protection

Administered by 'Cloud' organization.

Only desktop devices and network connections remain 'in-house'.

Outsourcing Security?

Server/storage service organizations
The 'Cloud!'

Reminiscent of early days of EHR/HIE:

RHIO – Regional Health Information Organization

Data/Information "Bank"

Analogous to Monetary/Wealth Banks

'Cloud' Outsourcing

Do Cloud Organization analysis carefully!!

This may require IS technical and network expertise!

A 'Culture of Security'

Building the C.O.S.:

- Understand the Hacker culture!!
- Awareness *and Responsibility* training
- Technical/Security expertise still needed
- Consider 'Cloud' vendors
- Don't wait!