COMPLACENT COMPLIANCE

Brian A. Engle

November 2, 2012

Agenda

- Teach Security
- Teach Christ
- Teach Security in Christ

About me…

- Chief Information Security Officer at Texas Health and Human Services Commission
- Past president and lifetime Board of Directors Member – ISSA Capitol of Texas Chapter
- ISACA Member
- CISSP
- CISA
- 13 years in Infosec and over 20 years in IT

About me…

- Vile, wretched, unworthy and worst of sinners
- Ill equipped to teach, and not the role model I would hope to be
- Prideful, selfish, gluttonous, envious – on my best days
- In need of constant grace, mercy and forgiveness
- Blessed and thankful

Not about me…

He must increase, but I must decrease.

John 3:30

Proverbs of another sort

Tell you, you'll forget.
Show you, you'll remember.
Involve you, you'll understand.

Challenge you, you'll desire to learn.

History of Compliance

Compliance:

The result of a failed risk assessment.

History of Compliance

Pharisees:

The first auditors.

Compliance Evolved

- Environmental Protection Agency Guidelines
- Occupational Safety and Health Administration
- Generally Accepted Accounting Principles
- Fair Trade Act
- United States Antitrust Law
- Federal Trade Commission Consumer Protection
- Federal Communications Commission
- Trade Associations

Compliance Applied

- Sarbanes-Oxley
- Gramm Leach Bliley Act
- Federal Information Security Management Act
- Health Insurance Portability and Accountability Act / Health Information Technology for Economic and Clinical Health Act
- Numerous State criminal, health, business and commerce laws

Why Compliance is Not Enough

- Limited in scope
- Single point in time
- Past tense and outdated
- Watered down and negotiated to approachable
- Lobbied to provide for special interests
- Rigid and inflexible
- Or worse, nebulous and vague

Securely Compliant

Compliance is the perfect security level…

Securely Compliant

Compliance is the perfect security level…

when your adversary is the auditor.

Securely Compliant

Compliance is the perfect security level…

when your adversary is the auditor.

Scheduled

Documentation is a valid countermeasure

Honors your data classification scheme, asset values and risk posture

Only 10

10 commandments yet still disobedient

But which is the greatest…

Love the Lord your God with all your heart and with all your soul and with all your mind. This is the first and greatest commandment. And the second is like it: Love your neighbor as yourself.

Matthew 22:37-39

Defiantly Compliant

- What is it about mankind that causes us to continue to push the limits?
- Skirt the edge, do the minimum, extend the minimal resources and expense
- Extend deadlines and procrastinate

Religious Compliance

- It's just a little white lie
- No one really got hurt
- Everyone does it
- I'll make up for it and do better tomorrow
- Seems wrong, but it's not a commandment
- Or isn't specifically referenced in the Bible

Religious Compliance

- Catholic Church divides sin into two categories plus the consideration of "7 deadly sins"
  - Venial Sin (minor guilt)
  - Mortal Sin (more severe)

It's a good thing that God is not an auditor, and not keeping score

The Role of Risk

Measured Risk?

Deferred Judgment?

Underestimated

Temporary

Unfeared Repercussions?

Instant Gratification?

Christian Security Professional

- The Christian life is not hard to live…it's impossible (David J. Stewart)
  - Judgment, Hypocrisy, Guilt…
- Can 'Security' ever be achieved?
  - Unrealistic expectations, difficult metrics, impossible goals
- Security Burnout
  - Judgment, Hypocrisy, Guilt… Eat our own young

With so much difficulty, how can we persist yet alone succeed?

Not Alone

- Community efforts and organizations
- Standards and consistency
- Sharing realistic 'Best Practices'
- Pragmatic, real risk based approaches
- Collaboration with colleagues
- Information sharing
- Healthy sense of humor

Through faith

For it is by grace you have been saved, through faith - and *this is not from yourselves*, it is the gift of God - *not by works*, so that no one can boast .

For we are his workmanship, created in Christ Jesus *for good works*, which God prepared in advance for us to do.

Ephesians 2:8-10

Work for the Lord

Commit your works to the Lord, And your thoughts will be established.

Proverbs 16:3

Vanity of vanities, says the Teacher; vanity of vanities, all is vanity. What profit has a man from all his labor in which he toils under the sun?

Ecclesiastes 1:1-3

The Armor of God

Finally, be strong in the Lord and in His mighty power.

Put on the full armor of God, so that you can take your stand against the devil's schemes.

Ephesians 6:10-11

Thank You!

Contact Info:

Brian.Engle@gmail.com

@brianaengle

www.infosec-land.com