WELCOME TO SECURE360 2013

- Don't forget to pick up your Certificate of Attendance at the end of each day.

- Please complete the Session Survey front and back, and leave it on your seat.

- Are you tweeting? #Sec360


SECURE360
conference
DAVE FUGLEBERG, CISSP, CISM
DEFENDER OR DECORATION?
TUESDAY, MAY14, 2013 - 2:25 PM

OBLIGATORY AGENDA SLIDE

Decorating the Data Center

Security Theatre

Who are you fooling?

Four Critical Mistakes

Stop the Insanity !

What could Possibly Go Wrong?

Taking it Personally

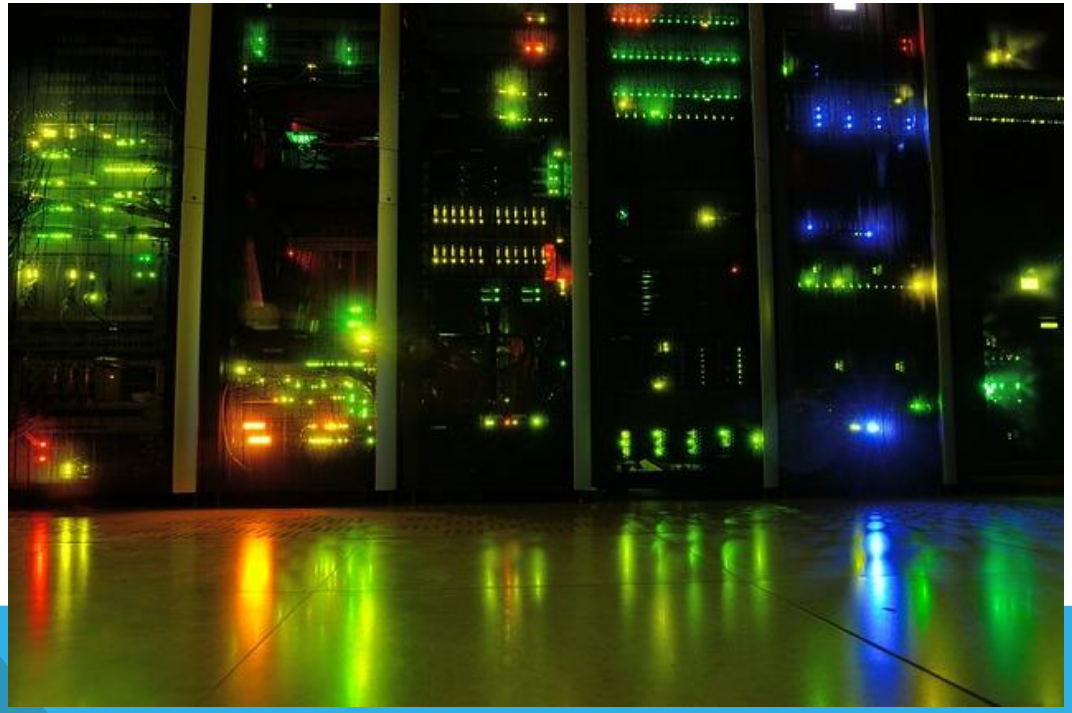
Dude, Where's My Controls?

Is this thing on?

Beyond the Checkbox

DECORATING THE DATA CENTER

- **Global Cyber Security Market > $55 Billion in 2011 (Gartner)**
- **32% of companies spend > $1M annually on information security (E&Y)**
- **Much of this money is wasted**



SECURITY THEATRE

- **Lights are on, but nobody's home**
- **The key is under the mat**
- **But, we have firewalls !**
- **Set it and forget it**
- **Trust us - we use Military Grade encryption**

Image courtesy of digitalart / freedigitalphotos.net

WHO ARE YOU FOOLING?

Adversaries?

Your boss?

Auditors?

Yourself?

Image courtesy of Renjith Krishnan/ freedigitalphotos.net

FOUR CRITICAL MISTAKES

Many (most?) issues with ineffective security controls can be traced to one of these four mistakes

Independent of product or vendor

Recognizing these mistakes can help you avoid them

CRITICAL MISTAKE #1 – "SECURITY" FOR ALL THE WRONG REASONS

- **Selecting "solutions" without understanding the problem**
- **"Best Practices"**
- **Because we can**
- **Checking the box**

Image courtesy of Stuart Miles/ freedigitalphotos.net

CRITICAL MISTAKE #2 – FAILURE BY DEFAULT

- **Things seldom work 'out of the box'**
- **Defaults can be dangerous**
- **Failure to properly configure**
- **Options Overload**
- **Inertia & Laziness**

Image courtesy of kraifreedom/ freedigitalphotos.net

CRITICAL MISTAKE #3 – ANARCHY-TECHTURE

- **Isolation vs Integration**
- **Box of parts vs finely-tuned machine**
- **Doing things right vs doing the right thing**
- **Silo focus vs System focus**
- **Doing less with more**
- **Lack of Architecture**

Image courtesy of xedos4/ freedigitalphotos.net

CRITICAL MISTAKE #4 – LACK OF FOLLOWTHR

- **Lifecycle (mis)management**
- **No Process Ownership**
- **I want a puppy!**

Image courtesy of phonsawat/ freedigitalphotos.net

STOP THE INSANITY!

- **What did you expect?**
- **First Rule of Holes**
- **Define problems – don't let them define you**
- **Align security controls with business needs**
- **Prioritize people and process over shiny toys**

Image courtesy of Michal Marcol/ freedigitalphotos.net

WHAT COULD POSSIBLY GO WRONG?

- Realistically assess THREATS and RISK
- Understand BUSINESS DRIVERS
- Build, maintain, and live within a POLICY FRAMEWORK

Ensure Security Controls are selected for the Right Reasons

Image courtesy of Stuart Miles/ freedigitalphotos.net

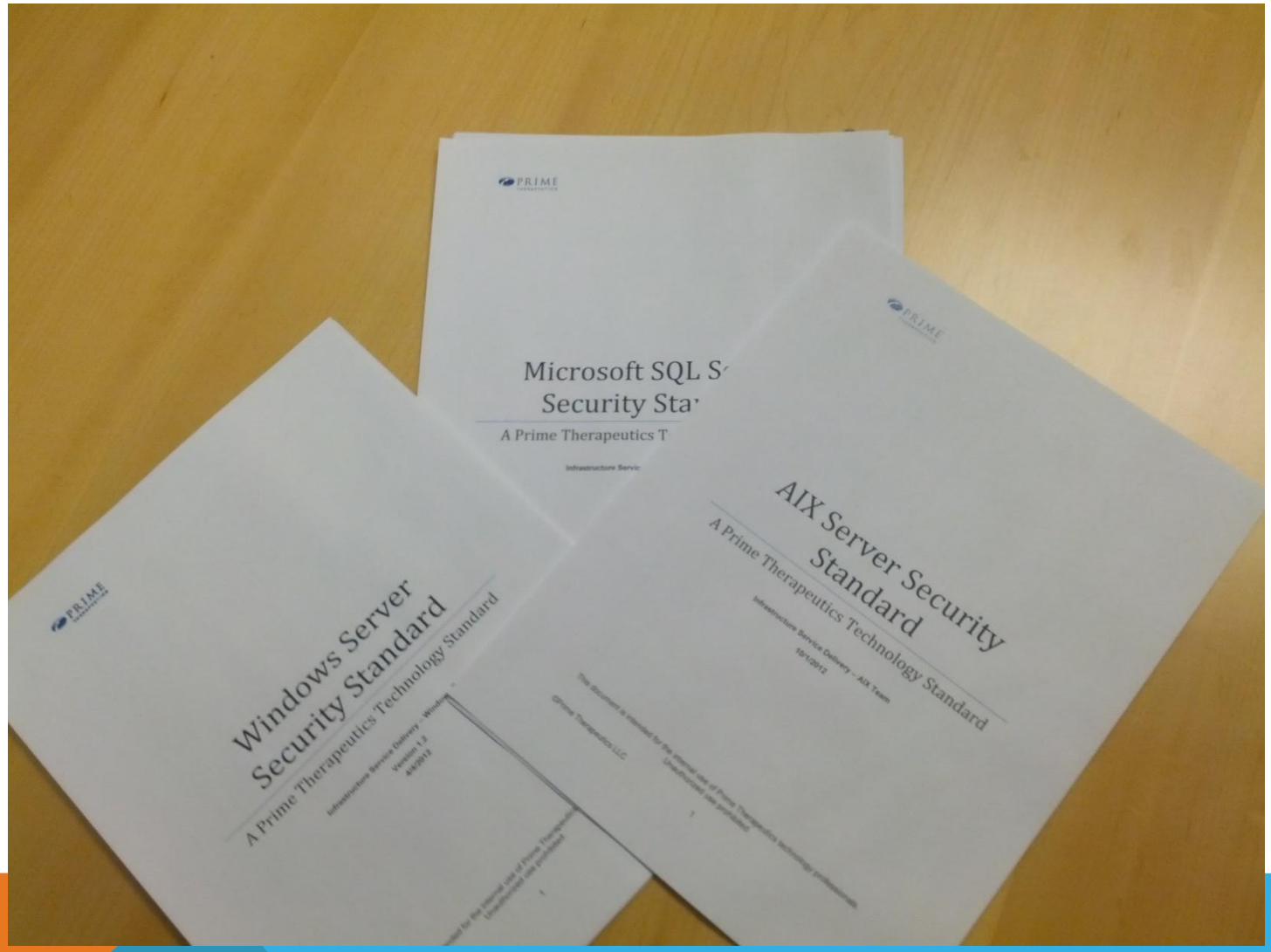

Growth
Client Contracts
New Markets
Health Care Reform
Regulations
Industry Certification

TAKING IT PERSONALLY

- **Document configurations and rationale**
- **Audit rules and settings**
- **Tailor to YOUR environment**
- **Reduce complexity**

Establish Defensible, Sensible, Repeatable Standards

Image courtesy of jannoon028/ freedigitalphotos.net

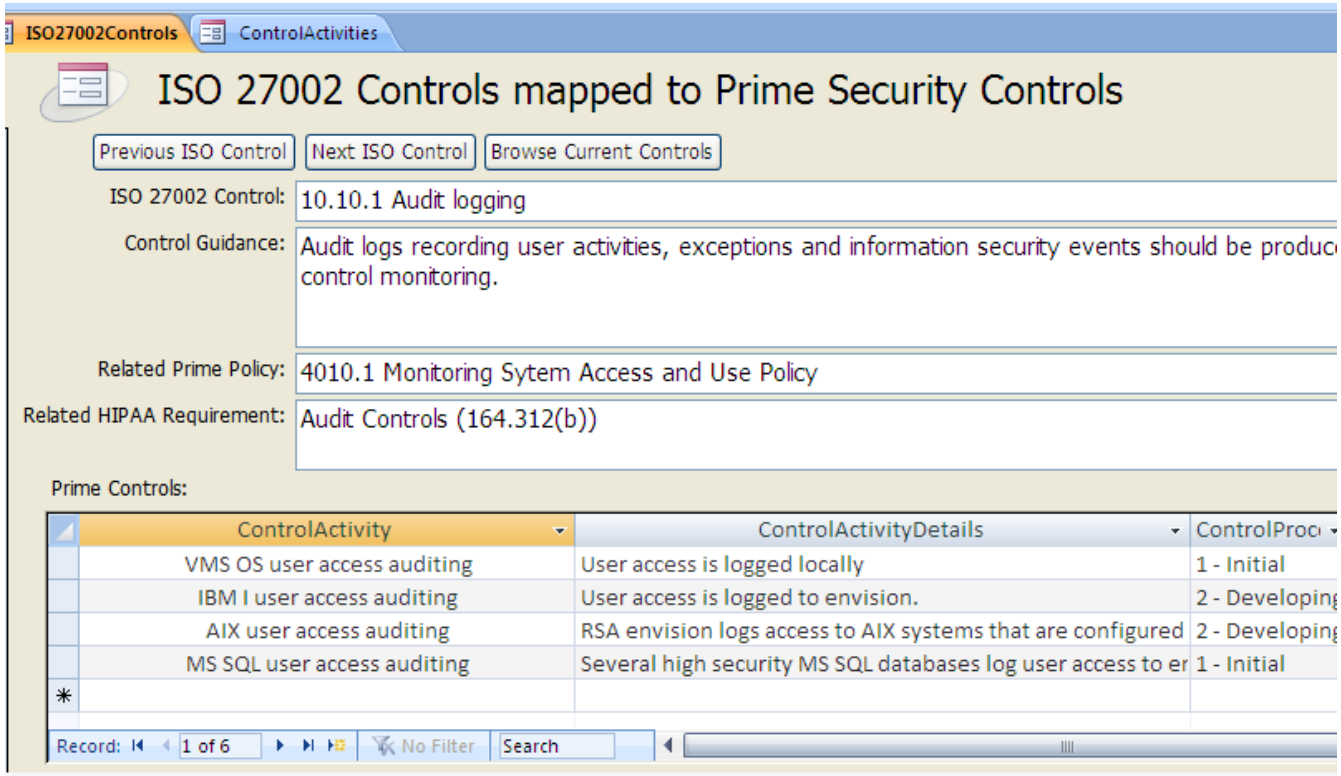

Windows Server
Security Standard
A Prime Therapeutics Technology Standard
Microsoft SQL S
Security Sta
A Prime Therapeutics T
AIX Server Security
Standard
A Prime Therapeutics Technology Standard

DUDE, WHERE'S MY CONTROLS?

- **Inventory existing controls**
  - What & Where are they?
  - Why are they needed?
  - Who owns them?
  - How are they managed?
- **Overlay controls on your enterprise**
  - Are they in the right places?
  - Are they aligned with risk?
  - Do they support the business need?

Security Architecture blends a diverse set of controls into a purposeful and cohesive whole

Image courtesy of Stuart Miles/ freedigitalphotos.net



Related PCI	ISO 27002 Control	Control Guidance
	10.2.2 Monitoring and review of third party services	The services, reports and records provided b G
	10.2.3 Managing changes to third party services	Changes to the provision of services, includi G
	10.3.1 Capacity management	The use of resources should be monitored, t G
2.1	10.3.2 Systems acceptance	Acceptance criteria for new information syst 4
5.1, 5.1.1, 5.2	10.4.1 Controls against malicious code	Detection, prevention and recovery controls 4

IS THIS THING ON??

- **Vital Signs**
  - Behavior
  - Diagnostics
  - Inspection
- **General Health**
  - Compared to baseline
  - Trending over time
  - Testing and probing
- **Operational Excellence**

Follow through with regular care and maintenance to ensure you're getting what you paid for

Image courtesy of stockimages/ freedigitalphotos.net

PRIME THERAPEUTICS

Table of Contents

BEYOND THE CHECKBOX

- **Map risks to control gaps**
- **Identify areas for improvement**
- **Use risk-based approach**
- **Pick the low fruit**
- **Make Mandates work FOR you**

Compliance does not always equate to security

Image courtesy of jscreationzs / freedigitalphotos.net

QUESTIONS?

Dave Fugleberg CISM, CISSP
Director, IT Security
Prime Therapeutics
dfugleberg@primetherapeutics.com