

3rd Annual E-Sec NW CIPS Summit
Doubletree Lloyd Center - Portland, OR
September 19th, 2007
Patrick C Miller CISSP-ISSAP CISA

The Business Case for Compliance

Why good security is good business...

Overview

- Regulatory Landscape
- Security Motivation
- Business Reasons For Compliance
- Financial Incentives For Compliance
- Closing Thoughts

I'm Not a Business Person, But...

Disclaimer...

- I have no formal business training or degree
- I have worked in the family business
- I have started my own successful business
- I have spent 7 years in Enterprise-class companies
- I have worked in multiple industry sectors
- I pay taxes and an electric bill
- I am a Security and Audit Professional: CISA, CISSP-
ISSAP, SSCP, NSA-IAM, SCP, TCP, etc...

Regulatory Avalanche

- CIPS
- AGA-12
- Sarbanes-Oxley
- HIPAA
- GLBA
- California SB1386
- FERC 888/889/890
- PDPSA/CPNI
- PCI
- CJIS
- MTSA (ISPS)
- SAFETY Act
- FIPS/FISMA
- 6 CFR Part 27

When Will The Dust Settle?

- When we resolve competing security standards that overlap or even conflict
- When Federal agencies producing these regulations can pass their own audits
- After strong legal precedents have been set (which means fines and lawsuits are inevitable)
- It will be a long bumpy ride, so make sure your seatbelt is buckled and *hang on...*

Security Motivation

- Terrorism, organized crime, hackers, skiddies...
- Corporate accountability fiascos, rampant ID fraud and data breaches - *ad nauseam*
- Budgets are only getting tighter; doing more work with less money
- Automation is everywhere; doing more work with fewer people; greater exposure
- Ever-increasing complexity, power and integration/interconnectivity
- “Good Utility Practice”

We've Never Been Hacked...

- So why do we need all of this protection?
 - I've never been hit by a car, but I still look both ways
- How do you know?
- Can you prove it?
- Do you own a home computer?
 - If so, do you protect it?
- Ever heard of TJX?

Security PR Bingo

<http://www.crypto.com/bingo/pr>

B I N G O				
WE'VE ALWAYS DONE IT THIS WAY	OUR SUCCESS SPEAKS FOR ITSELF	YOU DON'T UNDERSTAND THE CONTEXT	NO ONE WOULD EVER THINK OF THAT	NO COMMENT
WE TAKE SECURITY VERY SERIOUSLY	YOU'RE SO NEGATIVE	YOU'RE PARANOID	WE THINK IT IS SECURE ENOUGH	WE FOLLOW INDUSTRY STANDARD PRACTICES
WHAT DO YOU HAVE AGAINST US?	IF YOU HADN'T TOLD ANYONE, IT WOULD STILL BE SECURE	SECURITY PROBLEM EXCUSE BINGO	YOU'LL BE HEARING FROM OUR LAWYERS	YOU'RE BEING IRRESPONSIBLE
WE USE CRYPTOGRAPHY	WE HAVE CISSP CERTIFIED ENGINEERS	NO ONE HAS COMPLAINED BEFORE	NOBODY'S PERFECT	OUR PROACTIVE TECHNOLOGY SOLUTIONS PREVENT THAT
YOU ARE IN VIOLATION OF THE DMCA	WHAT KIND OF A PERSON LOOKS FOR FLAWS?	THAT'S JUST THEORETICAL MUMBO-JUMBO	LA, LA, LA WE'RE NOT LISTENING	WE MEET ALL GOVERNMENT STANDARDS

Automobile Industry Example

- Automobile safety push of the 1970s
- Happening again with Eco-issues
- A handful of companies change
- Some invested in change, before it was forced
- Huge market differentiator
- Highly successful results
- Those who changed early drove the industry

Energy Industry Difference

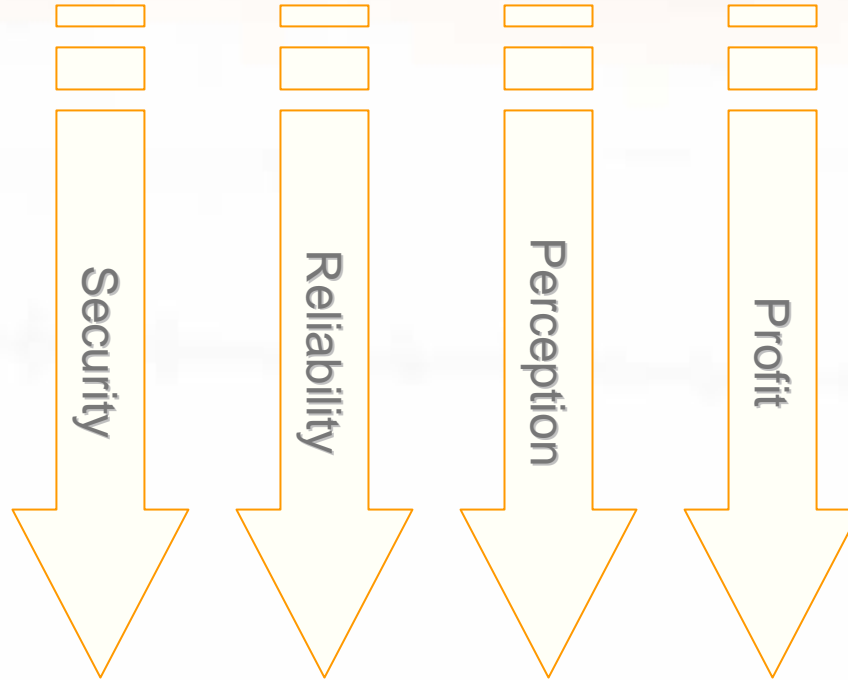
- If your customers are unsatisfied, they can't switch to a different company
- Since almost all aspects of the business are strictly regulated, it's all about the regulators, State and Federal...
 - PUC, PSC, CCB, CUB, etc...
 - FERC, NERC, RRO
- Being more (most) reliable is all we have

Happy Customers Matter

- Perception is 110% of reality
- Customer satisfaction is no small issue
 - Customers are represented by the State/Fed entities
 - If the State/Fed entities are unhappy, so are you...
 - Good security = good reliability
 - Good reliability = happier customers*
 - Happier customers = happier State/Fed entities
 - Happier State/Fed entities = better for your business

Reliability is only one factor influencing customer satisfaction...

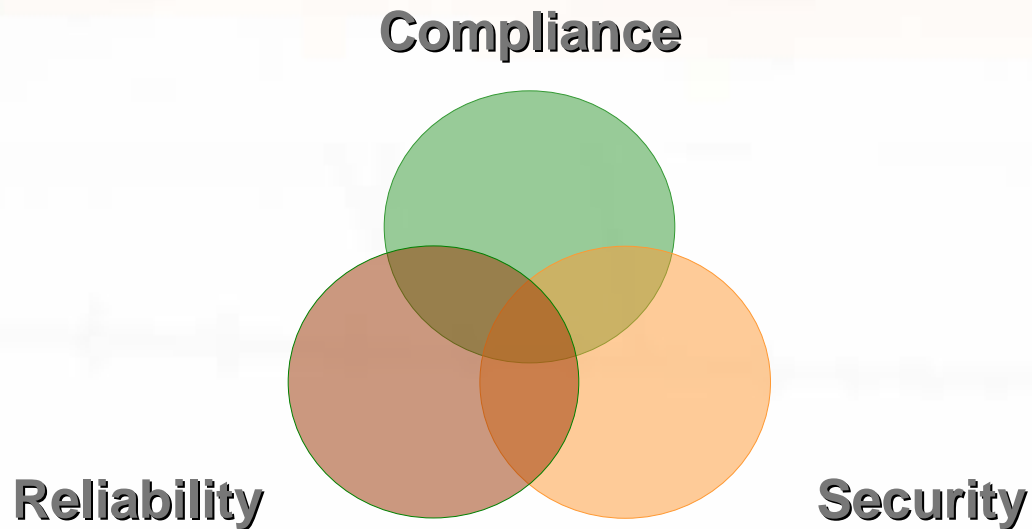
Simply Put...



Security ≠ Compliance

- An example: will the CIP standards protect you from metal theft? No...
- You can be very secure, yet not compliant
- You can be fully compliant, but still not secure
- Most regulations are the “low bar”
 - Only satisfy the most common scenarios
 - Do not speak to unique implementations
 - Often have the “gotta start somewhere” issue
 - One size fits most

The Ultimate Goal



No element trumps the others – they must all support each other

Put Your Money In Assets

- Much of the compliance effort may be rate-recoverable - NARUC even says so
- Security improvements are often “assets” which have a positive value on the books (and perception)
- Fines, sanctions and legal fees are negative value on the books (and perception)
- Which ultimately costs more: security or fines?

Scenario - If you didn't spend the \$\$\$ on security assets first, and you were fined as a result, then you get to spend the money on security AND fines, legal fees, etc...

Do It Right the First Time

- Touch each facility as few times as possible -- preferably just once:
 - Fewer trips will often mean fewer dollars
 - Piecemeal projects always cost more
 - Much easier on contracts
 - Greater chance of standardization
 - Improves consistency
 - Automate to reduce necessary headcount

One BIG Project Can Be Better

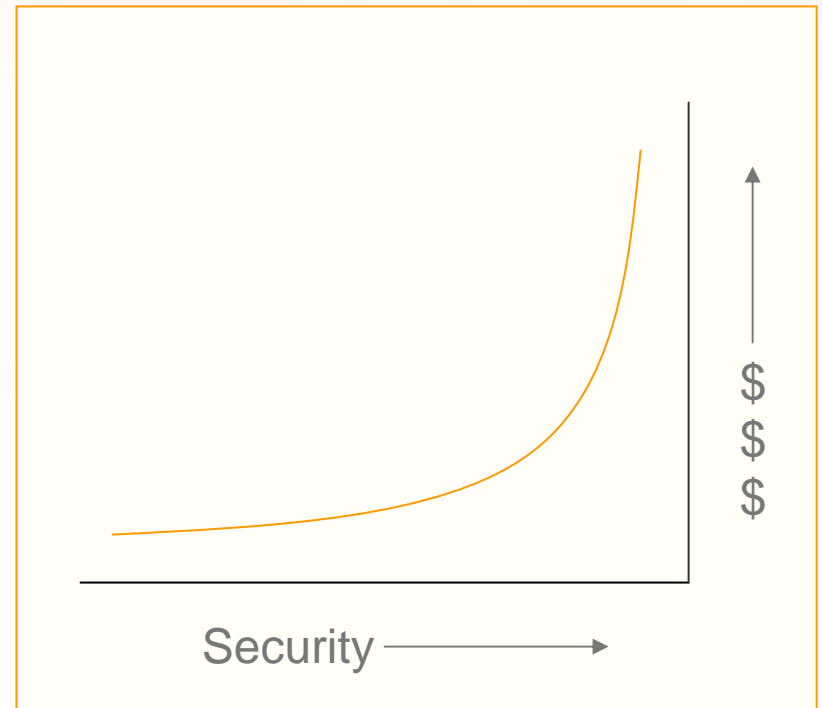
- Increases standardization and consistency
 - Easier maintenance
 - Easier auditability
 - Cheaper overall (proof: VisibleOps, ITIL)
- Better procurement and maintenance contract leverage
 - Volume discounts
 - Limited contractor availability
- Easier to track funding for recoverability
- Easier to demonstrate compliance plan

Plan Well and Spend Wisely

- Build security into the process ASAP
 - “A dime in development costs a dollar in production”
(1:10 planning principle)
- Bolt-on security after-the-fact will always cost more and be harder to maintain (inconsistent)
- Good security isn't cheap, so do your research
- Watch out for “snake-oil”, FUD and 100%
- Only buy stuff your staff can manage

Be Practical

- You don't have to "outrun the bear"
- The 80/20 rule
- Security is an asymptotic curve
- Nothing is 100% secure



Know Your Risks



- Ignoring risk is **bad** for your business, *whether intentional or inadvertent*
- Three risk options:
 - Accept (be careful)
 - Mitigate
 - Transfer
- Management owns risks

Go With What You Know

- You already have much of what it takes
- Piggyback on successful programs:
 - Safety
 - Environmental
 - Transportation
 - ITIL/ITSM (or CobiT, COSO, etc)
- You don't have to re-invent the wheel

Cashing In On Better Controls

- Better controls mean... (proof: VisibleOps)
 - Less unexpected change
 - Increased accuracy for root-cause analysis
 - Less system downtime
 - Increased productivity
 - Greater system-to-administrator ratio
 - Increased staff accountability
 - Less theft, resource mismanagement and fraud
 - Less time spent in audits/assessments

The Value of Awareness

- Security is a process not a product
- Israeli Airlines example
- United 93 effect
- The Aware Person System (APS)
- Training is cheap compared to technology
- Best way to change the culture

ROSI-Colored Glasses

- Higher likelihood of spotting bigfoot or aliens...
- Do you spend more on coffee or A/C than you do on security?
- Security is like insurance, you pay for it whether or not you actually use or need it
- Think of security more from a cost-avoidance or loss-prevention perspective instead
- Other metrics can be used to determine value

It's All About The Money, Right?

- What about the skilled workers needed to do the job? Will they be available?
- How are you recording all of your expenses? Did you design you program to be recovered?
- How much is too much? Even if the States/Feds allow the rate increases, what will the customer be willing to pay?
- Don't forget about grants...

Closing Thoughts

- You are part of the Critical Infrastructure... *Act accordingly and responsibly*
- “You’ve got to spend money to make money”; secure, reliable compliance is not cheap - but it can ultimately make you more profitable
- Security supports reliability and reliability supports your business; weak security will eventually translate into weak profit
- State and Federal laws are changing and you will eventually be forced to change with them; don’t wait to start compliance work
- Build appropriate security and controls into your everyday processes (both human and technological) and compliance will soon follow

Questions and Comments?

Patrick C Miller

CISA CISSP-ISSAP SSCP NSA-IAM

patrick.miller@pacificorp.com
503.813.7014