



The 21st Century CISO

Kim L. Jones

May 7th, 2008

Agenda

- **The Past**
 - **Security Career Pathing**
- **The Present**
 - **Trends and Challenges**
- **The Future**
 - **Possible End States**
- **Conclusions**

First, a Brief Disclaimer...

- I know exactly two things
 - My wife and son love me unconditionally
 - I could be wrong about absolutely everything else
- There are no definite conclusions to be drawn from this presentation...only questions and possibilities
- Some of the possibilities I'm presenting will disturb you...and well they should
- The purpose of this presentation is to make you *think about* and *engage* in the future of our collective profession

The Past – Security Career Pathing

“What Do You LIKE About IT Security?”

Playing with Technology

Making Money

Solving Problems

“What Do You LIKE About IT Security?”

Playing with Technology

R&D

- **Research University**
- **Chief Scientist**
- **FFRDC**
- **Advantages**
 - **Cutting Edge Problems**
 - **Cutting Edge Toys!**
- **Disadvantages**
 - **Degrees versus Certifications**
 - **Limited \$\$**

“What Do You LIKE About IT Security?”

Making Money

Product Creation/Business Owner

- **Consulting Partner**
- **Business Owner**
- **Advantages**
 - **Unlimited \$\$**
- **Disadvantages**
 - **Security Skills Become Secondary to Business Knowledge**

“What Do You LIKE About IT Security?”

Solving Problems

CISO

- **Advantages**
 - Good \$\$
 - Boredom? NOT!!
- **Disadvantages**
 - Ceiling on \$\$
 - Same problems, different companies.

Many Paths, Finite Destinations...

Playing with Technology

Making Money

Solving Problems

R&D

Product Creation/Business Owner

CISO

InfoSec Architect

ISSO

Sr. Infosec Engineer

Sr. Consultant/Consulting Manager

IT Auditor

Infosec Engineer

Consultant

Security Administrator

Firewall Engineer

Web Engineer

Network Engineer

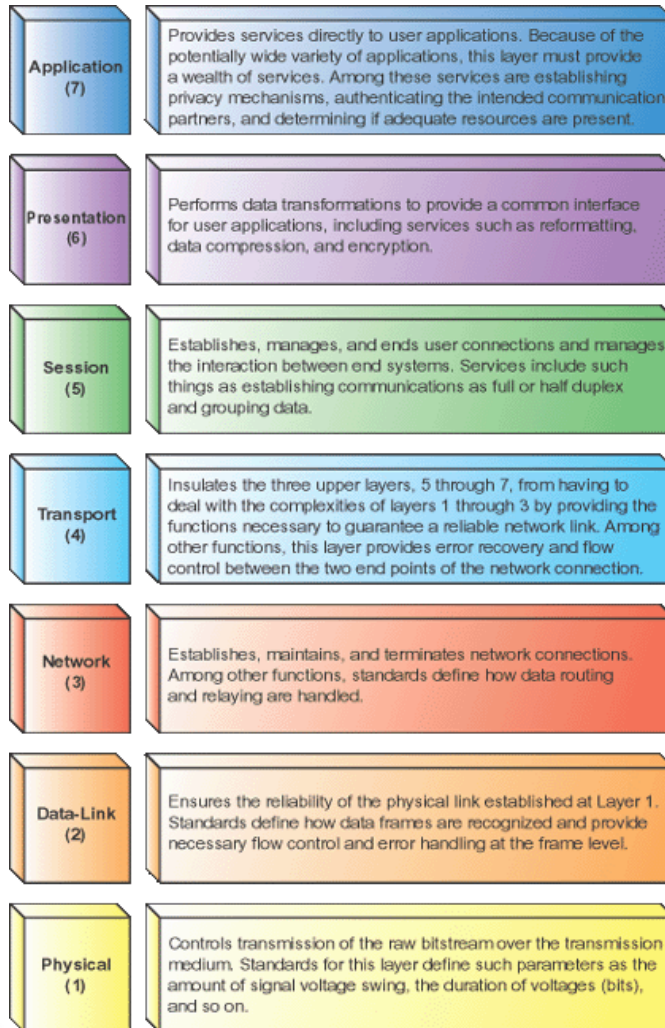
The Present – Trends and Challenges

Commoditization

- **Security tools and devices are becoming multi-functional**
- **Many sole-source tool providers combining/collaborating**
 - Lumension
 - Bladelogic
 - Symantec
- **Impacts**
 - More “one stop shopping”
 - Less integration issues
 - Less need for specialization?

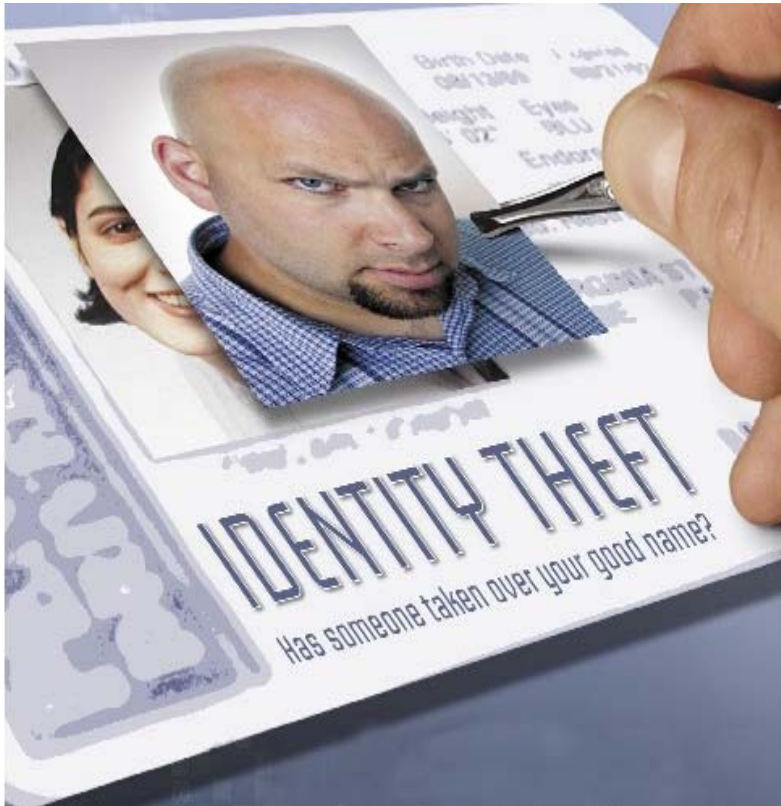


Protection Moving Up (Out of?) the OSI Model



- From network to application to *data*
- Impacts
 - Security (potentially) at more granular levels
 - More *expectations* of protection from our customers?

Data Losses



- **Choicepoint, TJ Maxx, Hanneford...the list goes on**
- **Impacts**
 - **Customer viewpoints on data becoming more stringent**
 - **Ambivalence decreasing...or is it?**

Security Regulations Increasing

- 38 state regulations
- Several regulations pending on a national level
- International regulations
- Impacts
 - More interest in security by the board room
 - “Security” now becomes “compliance?”
 - » Risk calculus being decided by lawyers?



Evolution of the Threat



- “Professionalization” of the threat
- Underground economy
- Have we evolved in kind?

Things to Consider

- Regulation *may* be considered symptomatic of an inability to self-regulate
 - BITS and PCI are trying to rectify this situation, but is it too little too late?
 - » Worse...enough/appropriate?
- We've yet to solve the metrics problem
 - Metrics measure against a standard...what's *our* standard?
- Are we an *industry* or a *profession*?
 - The answer, probably, is both...but are these at odds with one another?
 - » Standardization vs. “secret sauce?”
 - » “Cowboys” vs. licensing?

The Future – Possible End States

Option 1: “Chief Risk Officer”

- Security markets itself as a value-added service to the business
- Security expands its overall focus to encompass multi-faceted risk issues
 - Compliance?
 - BCP/DR?
 - Physical Security?
- Advantages are many
 - Holistic approach to risk (which should be the goal of any security/assurance professional)
 - Continued seat at the table
 - Numerous opportunities to expand outside of risk arena
 - » This approach mandates a detailed understanding of the business and positions you for non-risk related growth opportunities (CIO? COO?)
- Disadvantages
 - Forces a more meticulous understanding of the business that your security professionals might not have
 - Skillset requirements beyond the “normal” skillsets most junior security professionals have
- This is the option we are most comfortable exploring/discussing as a profession – because it is the most “appealing”

Option 2: Professionalism

- **Create and enforce standards of practice within industry**
- **Standard metrics and measurement**
- **Formal standards of conduct and requirements to enter – and practice – in the industry**
- **Advantages**
 - **Credibility?**
 - **Lack of ambiguity to business?**
- **Disadvantages**
 - **Enforcement?**
 - **Utility?**
 - » **May be more self serving an approach than a useful one**

Option 3...



Option 3: The CISO Becomes Obsolete

- Security becomes an integral a part of the operations framework (“Dial tone”)
 - “Secure operations” becomes a redundant term...though the term “secure” may become a pseudonym for “compliant.”
- CIO makes security risk decisions as s/he makes any other risk decision in the IT environment
- CISO title/position goes the way of the VP of Telephony

So...what does this mean to *you*?

So...what does this mean to *you*?

- At this rate, we have 5-10 more years of “status quo.” At that point, we will see our profession fundamentally changed
- The three options discussed are not the only ones out there
 - Remember the 2 things I know
- **THINK** about your future – and the future of **OUR** industry/profession
 - Educate those who work for you
 - Shape the dialogue
- **EXPAND** your views/horizons beyond security to the business

Questions??