Security Heretic: We’re Doing It Wrong

James Arlen aka Myrcurial
SecTor 2008
October 8, 2008
Hi.
Great title huh?
Disclaimer:

I am actively employed in the Infosec industry, but not authorized to speak on behalf of my employer.
Disclaimer:

I am actively* employed in the Infosec industry, but not authorized to speak on behalf of my employer.

* (I hope...)
Disclaimer (2):

I am going to say some startling things. There are no sacred entities when the heretic starts ranting.
Disclaimer (3):

If you are easily offended, you might want to get yourself a cool compress or some sort of smelling salts, it’s going to be a stressful hour.
Heretic

Her"e*tic\, n. [L. haereticus, Gr. ? able to choose, heretical, fr. ? to take, choose: cf. F. h[e]r[e]tique. See Heresy.]

1. One who holds to a heresy; one who believes some doctrine contrary to the established faith or prevailing religion.
I’m tired of looking silly.
Really tired.
Security “Industry” =
We can change that.
We can change that. We can fix that.
We can change that. We can fix that.

But it’s going to really irritate people.
We can change that. We can fix that.

But it’s going to really irritate people.

In a good way.
The Past
"Those that fail to learn from history, are doomed to repeat it."

- Winston Churchill
Information Security

» Confidentiality
» Integrity
» Availability
Julius Caesar: Mr. Confidentiality
Sumer: Integrity
Jewish Scribes: Availability
» Guilds
» Seals
» Obfuscation
» Physical security
Computer Security
» Theories
» 1970s
» Multics
» US Military
» Cambridge University
» Research Microkernels
The Religion
Religion

Re*li"gion\ (r[-e]*l[i^]j[u^]n), n. [F., from L. religio; cf. religens pious, revering the gods, Gr. 'ale`gein to heed, have a care. Cf. Neglect.]

4. Strictness of fidelity in conforming to any practice, as if it were an enjoined rule of conduct. [R.]
Best Practices
Common Practices
Habitual Responses
Insanity: doing the same thing over and over again and expecting different results.

- Albert Einstein
Certifications

- GIAC Certified ISO-17799 Specialist (G7799) - GOLD
- GIAC Certified ISO-17799 Specialist (G7799) - SILVER
- GIAC Assessing Wireless Networks (GAWN) - GOLD
- GIAC Assessing Wireless Networks (GAWN) - SILVER
- GIAC Certified Forensics Analyst (GCFA) - GOLD
- GIAC Certified Forensics Analyst (GCFA) - SILVER
- GIAC Certified Firewall Analyst (GCFWA) - GOLD
- GIAC Certified Firewall Analyst (GCFWA) - SILVER
- GIAC Certified Intrusion Analyst (GCIA) - GOLD
- GIAC Certified Intrusion Analyst (GCIA) - SILVER
- GIAC Certified Incident Handler (GCIH) - GOLD
- GIAC Certified Incident Handler (GCIH) - SILVER
- GIAC Certified Project Manager Certification (GCPM) - SILVER
- GIAC Certified Security Consultant (GSSC)
- GIAC Certified UNIX Security Administrator (GCUX) - GOLD
- GIAC Certified UNIX Security Administrator (GCUX) - SILVER
- GIAC Certified Windows Security Administrator (GCWNA) - GOLD
- GIAC Certified Windows Security Administrator (GCWNA) - SILVER
- GIAC Information Security Fundamentals (GISF) - GOLD
- GIAC Information Security Fundamentals (GISF) - SILVER
- GIAC Information Security Officer (GISO)
- GIAC Information Security Professional (GISP)
- GIAC Legal Issues (GLEG)
- GIAC Net (GNET) - GOLD
- GIAC Net (GNET) - SILVER
- GIAC Operations Essentials Certification (GEOEC)
- GIAC Reverse Engineering Malware (GREM)
- GIAC Security Audit Essentials (GSAE)
- GIAC Security Essentials Certification (GSEC) - GOLD
- GIAC Security Essentials Certification (GSEC) - SILVER
- GIAC Secure Internet Presence (GSP) - GOLD
- GIAC Secure Internet Presence (GSP) - SILVER
- GIAC Security Leadership Certification (GSLC)
- GIAC Systems and Network Auditor (GSNA) - GOLD
- GIAC Systems and Network Auditor (GSNA) - SILVER
- GIAC Securing Oracle Certification (GSOC)
- GIAC Secure Software Programmer - C (GSSP-C)
- GIAC Secure Software Programmer - Java (GSSP-JAVA)
Proselytize

Pros*e*ly*tize\, v. t. [imp. & p. p. proselytized; p. pr. & vb. n. Proselytizing.]

To convert to some religion, system, opinion, or the like; to bring, or cause to come, over; to proselyte.

ISC2® Reaches 50,000 Certified Members Worldwide

Business Wire, July 16, 2007

Milestone Reflects Continuing Growth and Influence of Information Security Profession

PALM HARBOR, Fla. -- (ISC)²("ISC-squared"), the non-profit global leader in educating and certifying information security professionals throughout their careers, today announced it has
New certification to stress software lifecycle safety

Chuck Miller | September 26, 2009

The movement to create secure software received a boost with the launch of a new certification from (ISC)², a nonprofit leader in educating and certifying information security professionals.

The certification, called the Certified Secure Software Lifecycle Professional (CSSLP), is designed to validate secure software development practices and build expertise to address the increasing number of application vulnerabilities.
Three Additional (ISC)2(R) Certifications Now Qualify Under U.S. Department of Defense 8570.1 Mandate

CISSP-ISSAP(R), CISSP-ISSEP(R), CISSP-ISSMP(R) and Associate of (ISC)2 toward CISSP(R) Now Among the Few Credentials That Qualify Under Rigorous Directive Designed to Professionalize DoD's Information Security Workforce

PALM HARBOR, Fla., July 29, 2008 /PRNewswire via COMTEX/ -- (ISC)2(R) ("ISC-squared"), the non-profit global leader in educating and certifying information security professionals throughout their careers, today announced that the U.S. Department of Defense (DoD) has approved four more (ISC)2 designations that can be used to meet the criteria of the DoD Directive 8570.1.
SANS: Popular certifications don’t ensure security

Effective training emphasizes technical knowledge, survey says

By Michael Arnone
Published on January 9, 2006

Editor’s Note: This story was updated at 5:22 p.m., Jan. 9, 2006, to reflect that the SANS Institute is a for-profit institute. The story previously stated that it was nonprofit.

Many popular information technology security certifications don’t improve holders’ ability to ensure computer systems’ security, according to a new survey from the SANS Institute, a training and education organization for security professionals.
A security qualification is a must
Certification to reflect IT governance expertise

An international association will begin offering an exam this fall whereby technology professionals can earn a certification that recognizes their ability to bring governance principles in the way IT is managed in the enterprise.

Developed by the Information Systems Audit and Control Association (ISACA), the certification will reflect deep knowledge...
How many CPE hours will you gain for questioning your religion?
Information Systems Audit and Control Association

hereby certifies that

James Edward Arlen

has successfully met all requirements and is qualified as a

Information Systems Auditor

...
Actually, I’m claiming this presentation as CPE hours.

You should too.
Sshhhhh...

Maybe they won’t notice the topic.
The Vendors
Professional Services
Hardware and Software
Pundits and the Media
The Dogma
Dogma


3. A doctrinal notion asserted without regard to evidence or truth; an arbitrary dictum.

The iPod Data Thief
The Complex Password
“Blood on the Walls”
Metrics
The answer is “No”
No Personal Use
I’m only responsible for logical security
The Renaissance
Individual Contributions
Research and Development
Synthesis

Syn"the*sis\, n.; pl. Syntheses. [L., a mixture, properly, a putting together, Gr. ?, fr. ? to place or put together; sy`n with + ? to place. See Thesis.]

3. (Logic) The combination of separate elements of thought into a whole, as of simple into complex conceptions, species into genera, individual propositions into systems; -- the opposite of analysis.
Enlightenment
The Ninety-Five Theses
The Twelve Step Program
Reduced to 9 steps for irony.
1. Admitting the problem.
2. Admitting our complicity.
3. Reasserting ethics.
4. Regaining our self-respect.
5. Finding a new path.
6. Eating our own dog-food.
7. Re-discovering passion.
9. Owning the suck.
NOT: Pwning teh 5uC|<0rz.
That’s a different talk altogether.
Q & A

followup: myrcurial@100percentgeek.net
Credits, Links and Notices.


Thanks: My Family, Friends, and the SecTor Advisory Committee.

Sources: notations and copies of materials are embedded within “notes” of the PPT file.

Inspiration: coffee, omelets made by my lovely wife, Strattera, Club Mate, Information Society, NIN, altruism.

Constructed with: Asus eeePC 701, Firefox, Powerpoint, angst.