Paths to Creativity in Security Careers

Privacy, Security and Trust 2006

Dr. Gregory Newby
Arctic Region Supercomputing Center
University of Alaska Fairbanks
The Message

- Security is, fundamentally, adversarial. Our goal is to protect against various risks.
- One element of an effective security posture is to insure the people protecting against risk are able to predict and understand their adversaries’ actions.
- These people need to be as creative, skilled and innovative as their adversaries.
Who is this Guy?

- Research faculty member @ UAF, serving as Chief Scientist of ARSC
- Research activity in information retrieval
- Varied information security credentials
- Active in creative technical communities
- Literary / information outreach focus
Digital Literati

Photo: gbn with Michael Hart @ HOPE6
From the Abstract

“Courageous, creative, educated, empowered and experienced individuals are a key component to building adaptable and healthy organizations.” (gbn)

Three themes:
- The “hacker spirit”
- Understanding complex systems
- Creativity in the organization
The Hacker Spirit

- Bob Bickford, computer and video guru, defined the true essence of the hacker as “Any person who derives joy from discovering ways to circumvent limitations.”
- A key question for is whether hackers are working for you, or against you.
Encouraging pursuing employees with the hacker spirit
Confused about Hackers v. Crackers?

It’s no wonder. This TLC show mixes criminals, viruses and others.

Consider the social & technical changes over time that makes yesterday’s pranks today’s crimes.
What color is your Hat?

- Does it matter? Or does only your activity, and intentions behind your activity, matter?

- Orgs
  - HAL 2001, WTH, H2K, H2K2
  - SC|06, PST2006

- Certs
  - CISSP, SANS
  - Being “3|334” on the nets
Understanding Complex Systems

- For systems of significant size (such as the Internet, or an operating system), nobody can fully understand complex systems.
- So, we use models, we experiment, we think.
- Apply diversity in skill sets, knowledge, and methodologies.

Image: Mandelbrot detail
Puzzles

- Piecing together all aspects of security scenarios: tough
- Different areas of expertise required
- Build a multi-disciplinary team

Photo: Tablet of “Gilgamesh” epic
Addressing Complex Systems

- Can you insure adequate and diversified staffing and attention to information security environment?
- How can the technologists benefit from the domain experts, and vice-versa?
- What are some “best practices” that can help (such as encryption, backups, privilege separation, and logging)?
Creativity in the Organization

- Everywhere? Maybe not...
- **Good judgment** is still a key requirement
- Checks and balances are needed
  - Remember that most computer crime is committed by **insiders**

*Photo: Jeffrey Skilling (Enron) heading back to jail*
Tips for Students

- Be broad; Be deep; Be technical
- Develop good communication skills
- Develop good habits for time management, so you have ability to monitor information security events and study them
Tips for Employers

- Give attention to security
- Encourage everyone to play an active role in information security
- Provide ongoing training for all aspects of technology, including security
- Don’t marginalize security - make it a core activity
- Work to evolve a sound, secure organization
Tips for Information Professionals

- Take time to reflect on security issues for any application / product / activity
- Learn to work with others to assess security risks. Don’t be a lone wolf, or closed-minded
- Be user-friendly
- You’re the front line, the last bastion, and the only hope
Challenges with Creativity

- Schools tend to teach conformance, and reward compliance
- Thinking “outside the box” might be frowned upon
- Performance & outcomes-driven organizations have little patience for deep thinkers
- We’re often too busy to be as creative as we wish
  - How can you encourage creative thinking?
  - Is it obvious why this is key for information security?

Photo: Anyone you know?
Creativity in Information Security

- Put yourself in your adversary’s shoes
  - G.H. Mead: Humans are the animal with the ability to perceive the other’s self-model
- If monkeys can do it, so can security professionals!
  - Scenario planning
  - Penetration tests
  - Systems/code auditing
    - (If you don’t do these things, maybe your adversary will)

Photo: G.H. Mead (U. Chicago Library)
Take-Away points

- Security is hard, and requires multiple approaches (duh…)
- Waiting for other people to develop strategies for responding to attacks is risky
- Your security posture needs to envision potential attacks and attackers
- If your attackers are more creative than you, you might be in trouble.
  - Therefore, seek out and foster creativity in your information security organization
See ya on the trails…

Photo: gbn in TRDMA dog race (see stinkypup.net)