

Into the Breach – Transitioning info an infosec career

Ray Pompon, CISSP

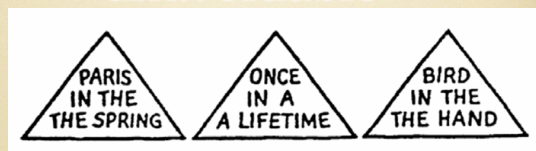
My journey

- High school -> Trash-80's, Apple2 and cracking
- Computer Science - Info Tech degree
- PDP-11/44 and this "Novell" thing
- LAN Admin at KPMG - soup to nuts
- Net integration firm - hooking orgs to "Internet"
- BECU - Net Engineer -> First security role there
- Security Architect at high-end security consultancy
- FBI's Operation Flyhook - undercover hacker
- ISMS Practice Manager - ISO27k work
- Security Officer at CapitalStream
- Director of Security at Linedata

What do IT engineers
struggle with the
most when going into
information
security?

Hint: it ain't the technology

"Mindsets are neither
good nor bad, but
they are
unavoidable"



Perception is framed by observer's
assumptions and preconceptions.

https://www.cis.sunyoh.edu/~mollan/teaching/cse591_visaanlytics/Visual%20Analytics%20-%20Chapter%202.pdf



Facilitating the business


Vs.


The Phoenix Project


"You win when you protect the organization without putting meaningless work into the IT system.

And you win even more when you can take meaningless work out of the IT system."

Advice to the security officer

<http://itrevolution.com/books/phoenixa-project-devops-book/>

50 shades of Risk



Vs.

Risk = Probability x Impact

What is business risk?

"Technology exists to further a business goal or objective. The failure of technology to perform as intended (i.e., technology risk) may result in or contribute to a business risk — the risk that business goals and objectives are not achieved effectively and efficiently."

GAIT Principles

https://na.thelia.org/standards-guidance/Publications/GAIT_for_Business_and_IT_Risk.pdf

Irony but realistic risk tradeoff



"A new car built by my company leaves somewhere traveling at 60 mph. The rear differential locks up. The car crashes and burns with everyone trapped inside. Now, should we initiate a recall?"

"Take the number of vehicles in the field, A, multiply by the probable rate of failure, B, multiply by the average out-of-court settlement, C. A times B times C equals X. If X is less than the cost of a recall, we don't do one."

[http://en.wikipedia.org/wiki/Fight_Club_\(film\)](http://en.wikipedia.org/wiki/Fight_Club_(film))

Infosec triad: C.I.A.

Data owners decide who gets to see their data (confidentiality)

Data owners decide who gets to modify their data (integrity)

Data owners will have access to their data when they want it (availability)

Think like a villain

•You will hear:
"But why would someone do that?"

•People who cannot imagine security failures, will not be able to avoid them



Trust

- People fail
- Technology fails (people made it)
- You will fail (you are a person)
- Everything is insecure until tested
- 50 shades of trust?
- Fail = doesn't conform to your expectations

Prepare for failure



- Nothing functional is impregnable
- We can never stop trying to improve
- What we "should be doing" is not enough

How do we fail successfully?

- Design with the assumption you will fail
- Under-promise and over-deliver
- Build defense in depth (not mono-cultures)
- Prepare an appropriate response
- Documentation of reasonable assurance
- Swift and transparent communication

Preso skills

- Explaining risk (analogy)
 - you will work with everyone in the company
- Presentation (writing, speaking, email) – be rational, be organized
- Providing assurance
- See the "trusted advisor" tutorial

Compliance

- What you need to do so you don't look stupid
- Liability, reasonableness, and TJ Hooper
- What are "best practices" for security ?
- Foundational standards

Legal things to know

- Compliance regs - HIPAA, SOX, etc.
- Industry compliance – PCI, OWASP
- Civil law – eDiscovery, Privacy, Contracts
- Computer Ethics
- Federal and State laws on data privacy
- Evidence collection
- Providing depositions (oral, written)

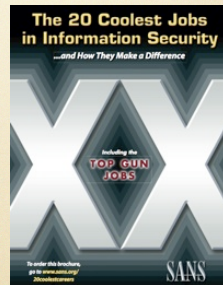
When looking at an audit report, remember

- They don't tell the whole story
- Tells a biased story
- Tells a limited story
- Tells a perishable story
- 50 shades of assurance?

All the previous skills
are essential for all
effective security
professionals

InfoSec Specialties

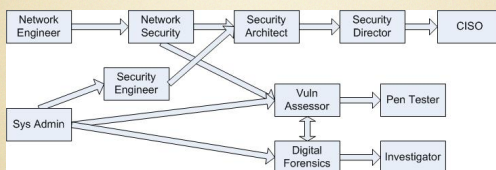
- Builder
- Tester
- Responder



SANS "Top 20"

Builder	Tester	Responder
Security Architect	System, Network, and/or Web Penetration Tester	Information Security Crime Investigator / Forensics Expert
Network Security Engineer	Application Penetration Tester	Forensic Analyst
CISO/ISO or Director of Security	Vulnerability Researcher / Exploit Developer	Incident Responder
Security-savvy Software Developer	Security Auditor	Malware Analyst
Security Maven in an Application Developer Organization		Computer Crime Investigator
Technical Director and Deputy CISO		Prosecutor Specializing in Information Security Crime
Security Analyst		Intrusion Analyst
Security Operations Center Analyst		Disaster Recovery / Business Continuity Analyst / Manager

Common paths



Or any other way you find works for you

Security Sales Engineering or Consulting

- Good customer service skills
- Good architecture and troubleshooting skills
- Lots of travel
- Highly focused (i.e. firewalls, PCI)
- Consultant-style work (rarely "own" a problem)
- Very high pay

Next steps

- **Certifications** - CISSP is universally accepted
- **Training** - SANS, local groups
- **Education** - UW has great classes
- **Networking** - Agora is best place to begin
- **Books and more** - See my blog for linkage
- **Make a career plan**

Questions

- Ray@huntingpompon.com
- @dunsany
- <http://assumebreach.blogspot.com/2013/03/cascadiait2013.html>