

Security, Stupidity and Employability

Alex Muentz

Quahogcon 2010

What this talk is about

- Staying curious
- Staying employed
- Relevant law
- A few case studies
- What are they afraid of?

Disclaimer

- While I'm an attorney
 - I'm not your attorney
 - Local laws and facts may vary
- I'm not HR
 - But I read their emails
- All the hypotheticals are based on real people
 - They've been obfuscated to protect the guilty
- This is a work in progress...

Terms for this talk

- Security Curious
 - IT/Physical security is only an interest
 - Not a part of your job description
- Security Conscious
 - IT/Physical security is peripheral to your job
- Security Responsible
 - IT/Physical security is core to your job

More terms

- 'Adverse employment action'
 - Demotion, firing, failure to hire
- Employment agreement
 - Vs contract
 - Vs employee handbook
- 'For Cause'
 - Discharge for breach of employment agreement

Employment law in a nutshell

- At will employment
 - Currently the law in all states but Montana
- Either party (employer or employee) can terminate the relationship
 - At any time
 - For any reason
 - Including stupid or incorrect ones
 - Or no reason at all
 - As long as it isn't an illegal one

At-will, continued

- Exceptions
- Employment contract
 - That disclaims 'at will'
 - Some states imply employment contracts
 - 'Good faith'
 - Union/Civil Service/Tenure

Wrongful Discharge

- This doesn't prevent firing
 - Just gives you the right to sue for damages
- 'Protected Class'
 - Sex, Race, Religion, Age > 40
 - Sexual preference in some states

Wrongful Discharge, cont

- Whistleblower protection
 - If informant reports to relevant agency
 - Not internal reporting
- 'Public Policy'
 - Refusing to commit unlawful/immoral act
 - Or retaliation for doing civic duty

Worldview(s)

- Geek
 - Barriers are to be overcome
 - They get in the way of work
 - More eyes find issues faster
 - Reduce risk
 - Let's all help out!

Worldviews, (cont)

- Lawyer/HR
 - Barriers keep us safe
 - Policy/procedure driven
 - Stay in your fucking box
 - Very risk adverse
 - About known/knowable risks
 - Sometimes to excess
 - Failing while doing everything right is OK

Risks perceived by employers

- Institutional integrity
 - HR & IT departments keep secrets and enforce
 - You're a threat to that (even when you're not)
 - Legal liability
- You're not exploring for fun
 - Dry run for theft or fraud
- It's a nice way to fire you for cause

Case Studies

- Vinnie
 - Works for IT consulting firm
 - As IT analyst/security consultant
 - Security Responsible...
 - Goes to hacker conference
 - Discloses security issue with client
 - (client happens to be at conference)
 - Another attendee overhears and makes a few calls
 - Now Vinnie is unemployed.

Ralph

- Customer service/tech support contractor at ISP
 - Security curious and ambitious
- Notices a security hole in an application
 - Can easily obtain HR info w/o password
 - Verifies extent of issue
 - Reports to his (supportive) supervisor
 - Fired for his efforts

Bob

- Works as a contract employee for a law firm
 - Not curious at all...
- Inadvertently clicks on wrong link
 - Outlook web mail
 - Has global access to very sensitive data
 - HR, billing, perhaps email?
 - Informs security conscious cow-orkeer

Sid

- Sid is IT guy at branch office of retail chain
 - Security aware
 - Security responsible IT staff are at HQ
 - Identifies issue with system that touches CC payments
 - At an inopportune time (layoffs)
 - HQ staff 'reframe' issue
 - Sid gets canned for 'causing' security issue

Takeaways

- Here's where it's better to ask for permission than forgiveness
 - Get it written into your job description
- Document everything
 - Permission, what you did and who you talked to
 - In case things get funny

Takeaways, continued

- If you are fired...
 - Consider the following:
 - Employment contracts still bind
 - Non Disparagement clause
 - Negotiated recommendation letters
 - Agreement to cooperate
 - Non disclosure/ non compete
 - Perhaps worth a quick consult