

➤ Information Security Decisions



Risk Management: Why It's Important to Know Your Adversary

Aaron Turner
Enterprise Security Partner
N4struct

Why Are We Here?

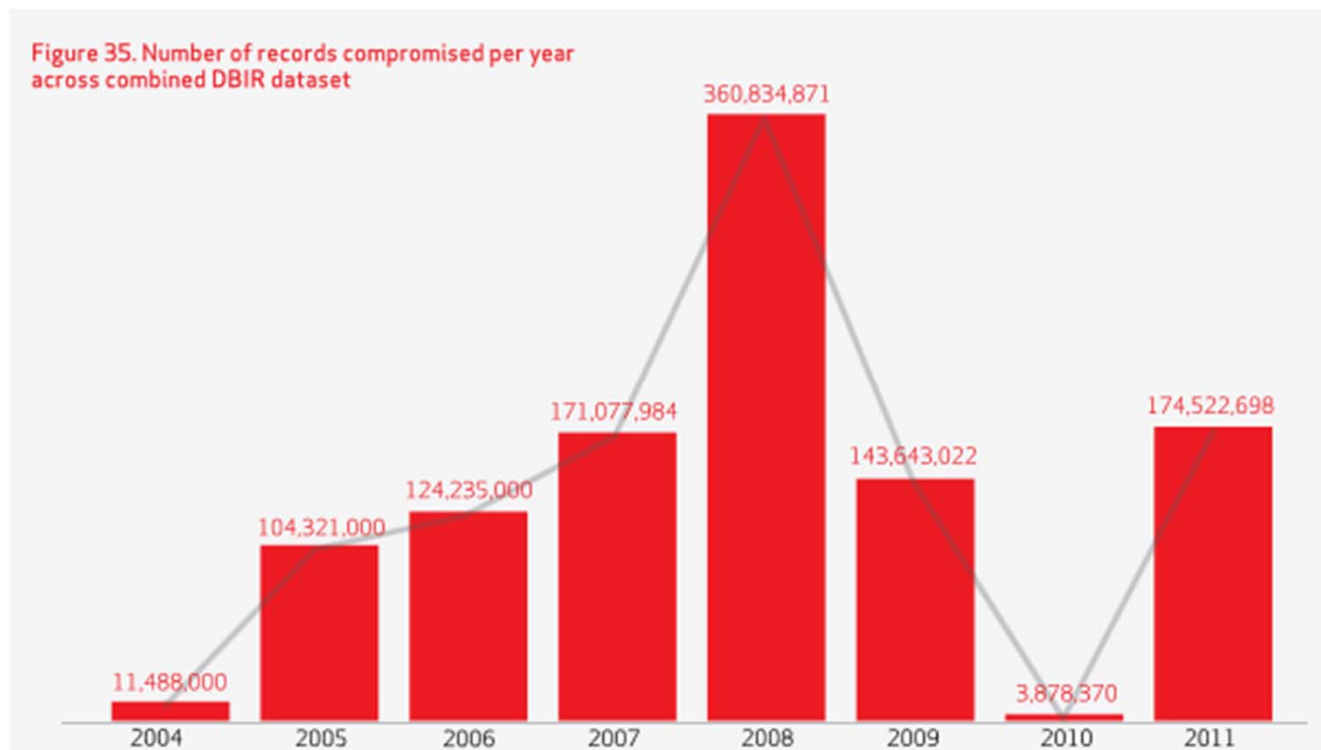
- You came to see me talk... So who am I?
- Relative effectiveness of Information Security
- Relative career satisfaction of InfoSec Professionals
- Industry acronyms I hate
- Who is on the other side of the looking glass?

Who is This Aaron Turner Guy Anyway?

- Long-time InfoSec... victim? ... participant? ... err...
- When non-technical friends ask me what I do for a living, I tell them that I'm an Internet Janitor & Hall Monitor
 - Clean up really big messes
 - Sometimes I've created big messes for the sake of testing out new kinds of cleaning supplies that we will need in the future
 - I've tried to track hackers and understand what they do and how they do it
- Involved in cleaning up some of the worst industrial espionage cases in the last 12 months

Relative Effectiveness of InfoSec Over Time

- Interesting but ultimately useless graph that shows we suck



From http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Relative Career Satisfaction of InfoSec Professionals

- 43% of CIO's believe they are 'Security Leaders' (2011 PwC & CSO Magazine Survey)

- 100% of CIO's believed they were responsible for protecting data of over 500 GB

- ~50% of InfoSec professionals are in Janitor jobs

- Quote of the year: "How much data we protect, it's really just about what the CIO *thinks* we're protecting." - Fortune 500 security team member



Janitor jobs
combined total

2011 Internet
e

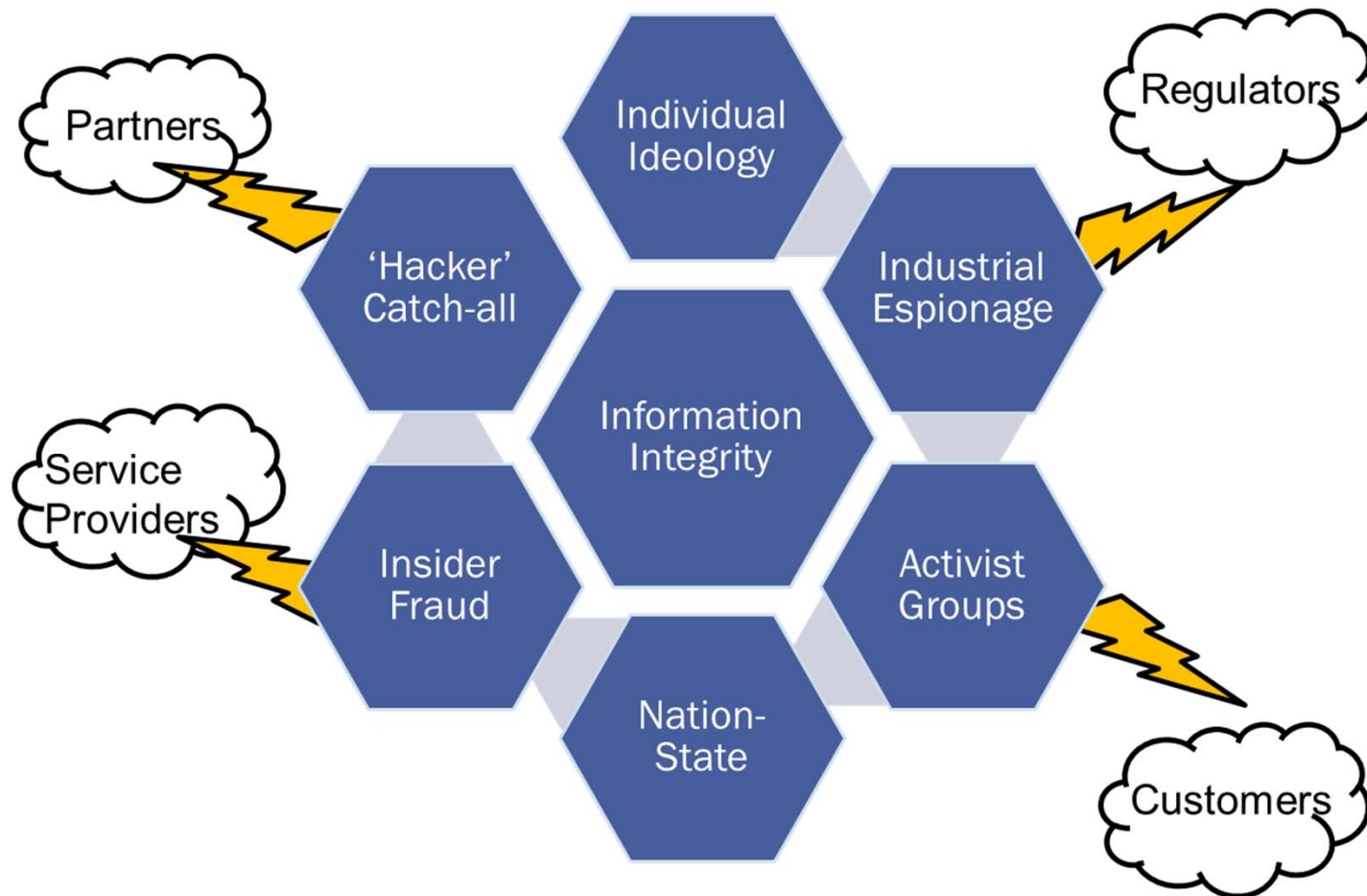
How much data we

The Industry Acronym I Hate

- APT
 - Brought to you by the US Military Branch that inspired Catch 22
 - Vendor buzz word which is now completely useless in describing anything related to Risk Management
- It's not the threat that matters my esteemed InfoSec marketing colleagues!
- It's the ADVERSARY!!!



Information Integrity Risk Factors



Root Cause Analysis of Cablegate/Wikileaks

- 251,287 cables consisting of 261,276,536 words (largest release of US Gov't Classified information ever)
- Facilitated by one individual – Private Bradley Manning
- Why?



Key to Success: Organizational Ideology

- How would you categorize your organization's ideology?
 - Is it trending a particular direction?
 - Are future product announcements/partnerships going to trigger ideological adversaries?
- Ideology is a powerful motivator for adversaries
 - Internal or External actors
 - Hacktivism has created economies of scale for new sub-culture of ideologically-driven information warfare
- Action Item: Weave PR's 'brand management' capabilities into InfoSec response plans

Professional Adversaries

- Organized-crime and state-sponsored attackers are professionals
 - Generally work a normal schedule
 - Hierarchical organization structure
 - Escalation paths to solve problems
- Low-level grunts do the drudgery
 - Scope out 'easy prey'
 - Can run command-line tools, but usually take several tries to get it right
 - Are often opening and closing help files
- Mid-level experts solve problems
 - Overcome security controls
 - Generally have a particular area of expertise
 - Quick and precise in their use of command-line tools
- Scary-smart geniuses who do real-time battle to get what they want
 - Design persistent means to fool even the best
 - Creative in their use of tools
 - Drive the team to efficiency and to look like they are 'victim admins' ASAP

One Case Study


- Attack began with spear-phishing
 - Attackers used list of industry conference attendees to get to those with the best information about a sensitive project
- Spear-phishing using XLS and PDF
 - Some attachments had redundant exploits (if patched for X, then run Y)
- Attackers quickly went for Domain Admin credentials
 - Gained access to all Domain Controllers & dumped password hashes for 9000 user accounts in matter of minutes
- Attackers setup their own file storage system
 - They ran out of space on the designated file servers, so they started looking for under-utilized servers
- Why bother dumping SAP credentials...
 - Attackers gained access to SAP backend Oracle system making it nearly impossible for company to certify their financials for year-end
- Slow MPLS lines to foreign countries made attackers impatient
 - Attackers installed wireless communications equipment capable of 5Mb/s speeds in and out of victim's facilities
- Attackers wanted trade secrets for new product
 - Gained access to the manufacturing control system network to get key intellectual property

Who Are These Guys?

- Outside of law enforcement, we don't have access to names, faces, work locations
- They're master craftsmen who are improving their trade
- Evidence suggests that some have worked in the past for their respective countries in military/intelligence roles
- More and more are entrepreneurs – lots of upside... what's the downside again?

What To Do?

- Evaluate your company's Ideological Footprint
- Keep penetration testing in place but it's time to innovate
 - Ever done an exfiltration test?
- Create a dialog with business leaders to understand true BUSINESS adversaries
 - Entering a new country? Developing a new product? Just hired a new CEO from a competitor?



Aaron Turner
Enterprise Security Partner
N4struct



Featured Member of the
TechTarget Editorial
Speaker Bureau