What the Security Profession Can Learn From the Intelligence Profession

Ira Winkler, CISSP

Codenomicon

Session ID: HT-208

Session Classification: General Interest

RSA CONFERENCE EUROPE 2012

Why This Presentation?

- Security programs rarely seem to have a proper focus
- They focus on threat, hype, and vendor pitchers
- They focus on the obvious
- Intelligence agencies have limited budgets, like all organization, but relatively few problems

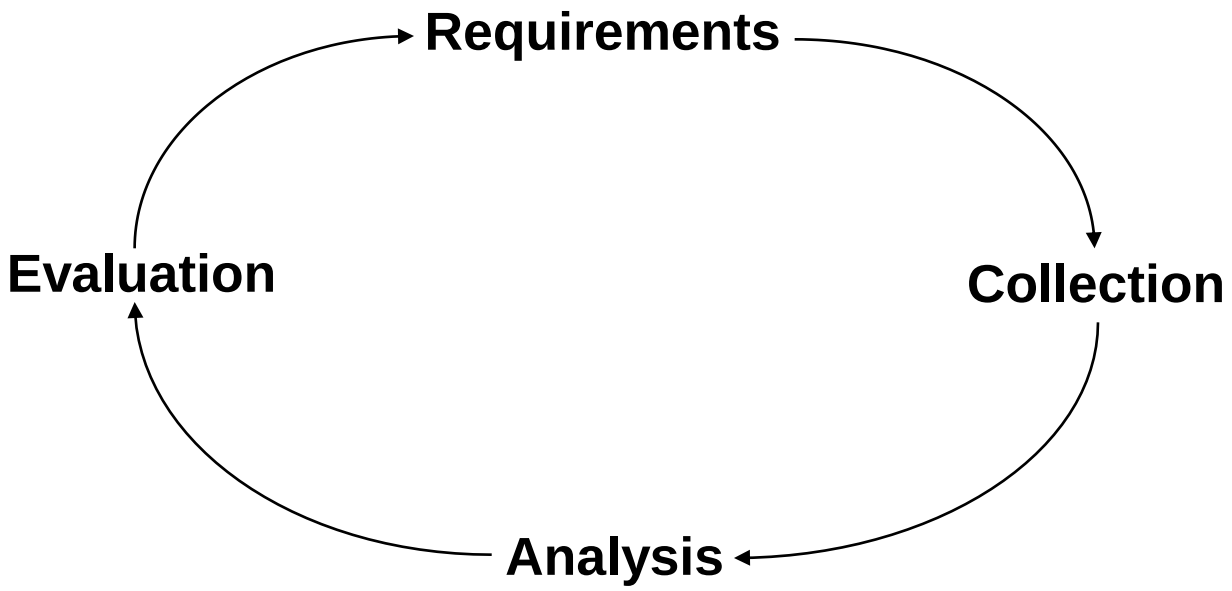
What Makes Intelligence Different than Security?

- Intelligence is the collection and analysis of an adversary's information
- Intelligence agencies have a process in place and train their employees in the process
- Security secures their organization
- Security programs generally lack a process

How is Intelligence Different than Hackers?

- Hacking is random
- The skill and methods of hackers varies greatly
- Hackers are opportunistic
- Intelligence collectors are chosen for their skills
- They are trained in a well established and coordinated process
- Collectors are generally well supported with other resources
- Targeting is usually well thought out

The Intelligence Process



Requirements are the Key

- Intelligence agencies have clear requirements
- These are their targets
- They drive the collection methods
- They are agnostic to the form the collection takes
- Therefore, the most effective collection method(s) are used

Types of Intelligence

- HUMINT
- SIGINT
- OSINT
- COMINT
- COMPINT
- PHOTINT
- TRASHINT
- MASINT

Never Relies on a Single Method

- Can be deceived from a single source
- SIGINT has proven to be the most reliable
- HUMINT can be the most sensitive and valuable
- Computers are becoming a major source of information

The Importance of Computers

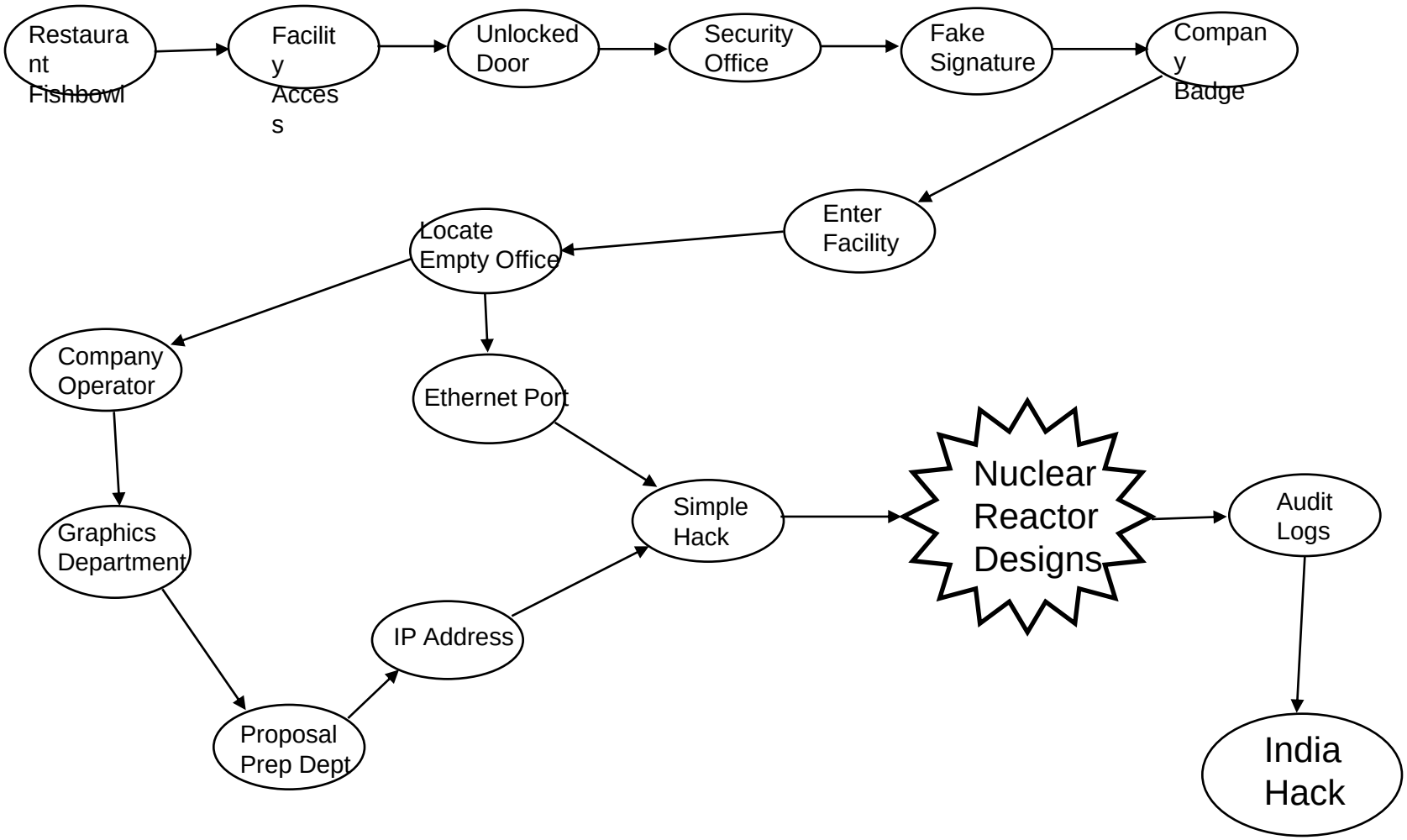
- Computers are a major source of information
- Computers provide valuable services
- However they are only valuable as they have information or services
- The key is finding the right computers

Case Study #1

- Compromise of nuclear secrets
- Full scale espionage simulation
- No holds barred attack
- Multi-faceted attack
  - Open source research
  - Misrepresentation
  - Walk through facilities
  - Internal hacking

Background

- Organization is very large with a large central organization
- Had traditional security issues, but no major issues that they knew about
- Organization as a whole experienced massive layoffs
- Only one security manager at HQ, with an intern, and no unit security managers


Restaurant Fishbowl
Facility Access
Unlocked Door
Security Office
Fake Signature
Company Badge
Enter Facility
Locate Empty Office
Company Operator
Ethernet Port
Graphics Department
Simple Hack
Nuclear Reactor Designs
Audit Logs
IP Address
Proposal Prep Dept
India Hack

Results

- Nuclear reactor designs compromised
- Emerging technologies compromised
- Production potentially compromised
- National security implications
- It was extremely simple
- ID card was unnecessary

Believe it or Not

- Critical compromises accomplished within a half day
- No reports of any activities
- India hack was previously unknown

Counterintelligence

- Traditionally counterintelligence focuses on knowing who the bad guys are and what they're up to
- It traditionally focuses on the Threat
- There is a Security group that focuses on generically protecting information
- Security focuses on Vulnerabilties

$$\text{Risk} = \left(\frac{\text{Threat} * \text{Vulnerability}}{\text{Countermeasures}} \right) * \text{Value}$$

Risk Broken Down

- Threat – Who or What is out to get you
- Vulnerability – Your weaknesses that allow the Threat to exploit you
- Value – Value of your information or services at risk
- Countermeasures – Measures taken to mitigate the Risk

Vulnerability is the Biggest Worry

- If a vulnerability exists, anyone can exploit it
- It doesn't matter who they are
- Exploitation could be planned, or an accident
- If a vulnerability doesn't exist, no threat can damage you

Counterintelligence vs. Security

- These are independent efforts
- They should work together
- Counterintelligence should help Security target their methods
- Security however doesn't need Counterintelligence

Intelligence Security

- Security has to be right 100% of the time, the bad guys have to be right just once
- Security focuses on identifying vulnerabilities
- Vulnerabilities are prioritized
- Vulnerabilities are remediated as prioritized

The Commercial World Confuses the Two

- The commercial world tends to attempt to address hackers, outsiders, competitors when creating security programs
- They cross the line between Threat and Vulnerabilities
- This confuses the issues and the priorities

The Ideal Security Process

- Identify vulnerabilities
- Determine the vulnerabilities that are most likely to be exploited
- Determine the costs of the exploitation of the vulnerabilities
- Determine the countermeasures and their costs
- Prioritize countermeasures to implement

Focus on Choosing Countermeasures

- A Security program is the implementation of countermeasures that mitigate vulnerabilities
- Countermeasures must be relevant to the vulnerabilities that exist within your organization
- Mitigating low “value” vulnerabilities does not significantly reduce your risk

How to Use Counterintelligence

- If you have specific details, knowing the Threat can help you determine which vulnerabilities may be exploited
- You may know their specific methods
- In the Intelligence world, there is a temporary focus on detection and certain relevant countermeasures with a known Threat
- It does not drive the Security program
- Could act as early warning

Countering Threat

- Some countermeasures do mitigate the threat
- Background checks, security patrols do work
- They are limited though

Threat is a Factor in Damage

- More sophisticated threats could cause more damage
- Less sophisticated threats could cause accidental or malicious damage, which results in more devastating losses
- More sophisticated threats will be harder to detect
- They still can only exploit the vulnerabilities that exist

Data Classification

- A key countermeasure is prioritizing the data to be protected based on value
- More valuable data gets more priority in funding countermeasures

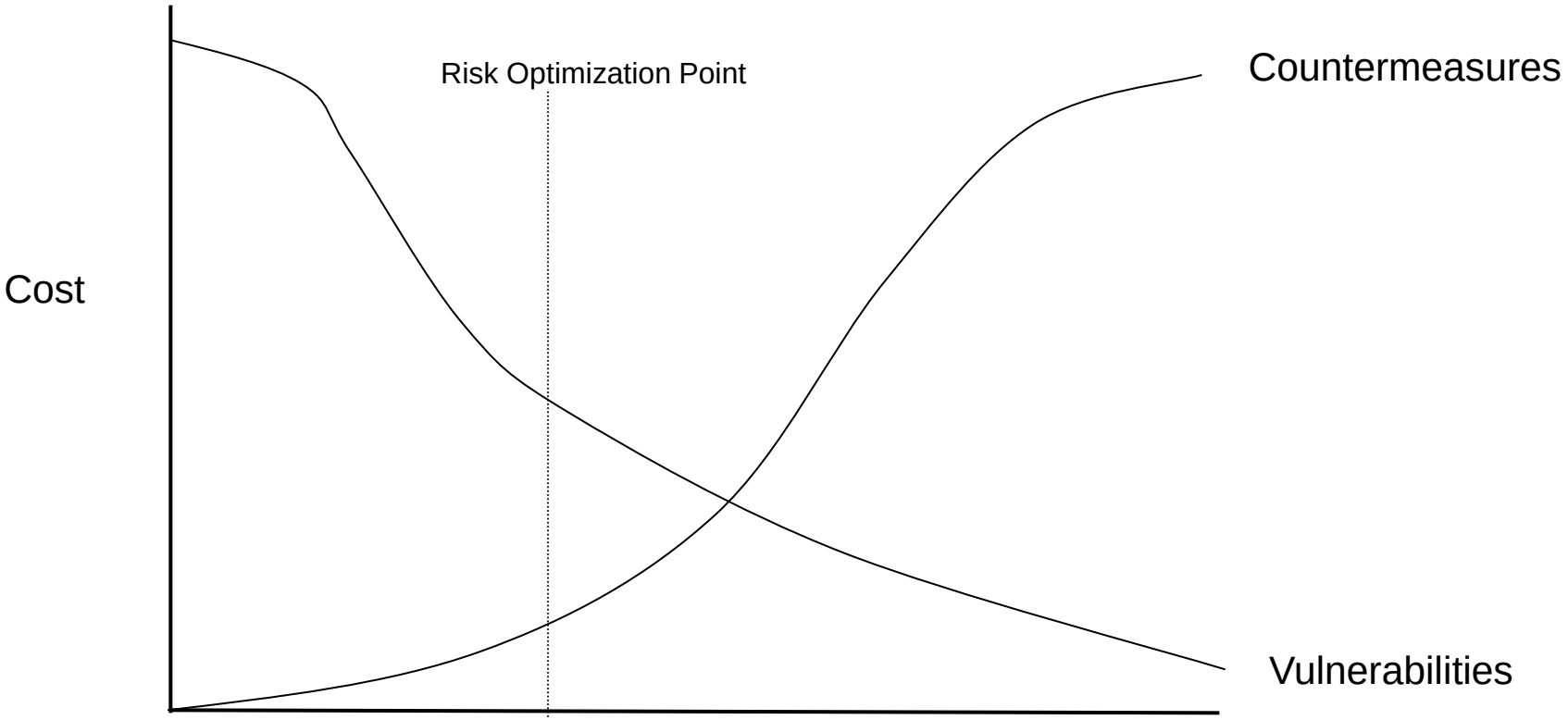
Defense in Depth is the Key

- Any single countermeasure can fail
- Any single countermeasure can be bypassed
- Many countermeasures stop multiple vulnerabilities
- Use the overlap as much as possible

Awareness Training

- The best countermeasure you can ever have
- Intelligence agencies start awareness training at day one, and reinforce it daily
- People need to know:
  - Their information has value
  - Someone/anyone will steal it if given any opportunity
  - They should report things
  - The countermeasures and how they work

Optimizing Risk



Potential Loss Should Drive Budget

- Most security programs are determined by money available
  - Risk is a result, not a consideration
- Security program budgets should be a factor of Optimized Risk
  - Risk is the driver for the budget
- Remember, there is a great deal of ROI for most Countermeasures
  - There are only two ways to hack a computer

Summary

- Countermeasures should not result from budgets and vendor hype
- Information and services focus, not computer focus
- There should be Defense in Depth
- You must focus on Countermeasures that mitigate Vulnerabilities
- Realistic security is achievable

For More Information

Ira Winkler, CISSP

ira@isag.com

+1-410-544-3435

@irawinkler

http://www.facebook.com/ira.winkler

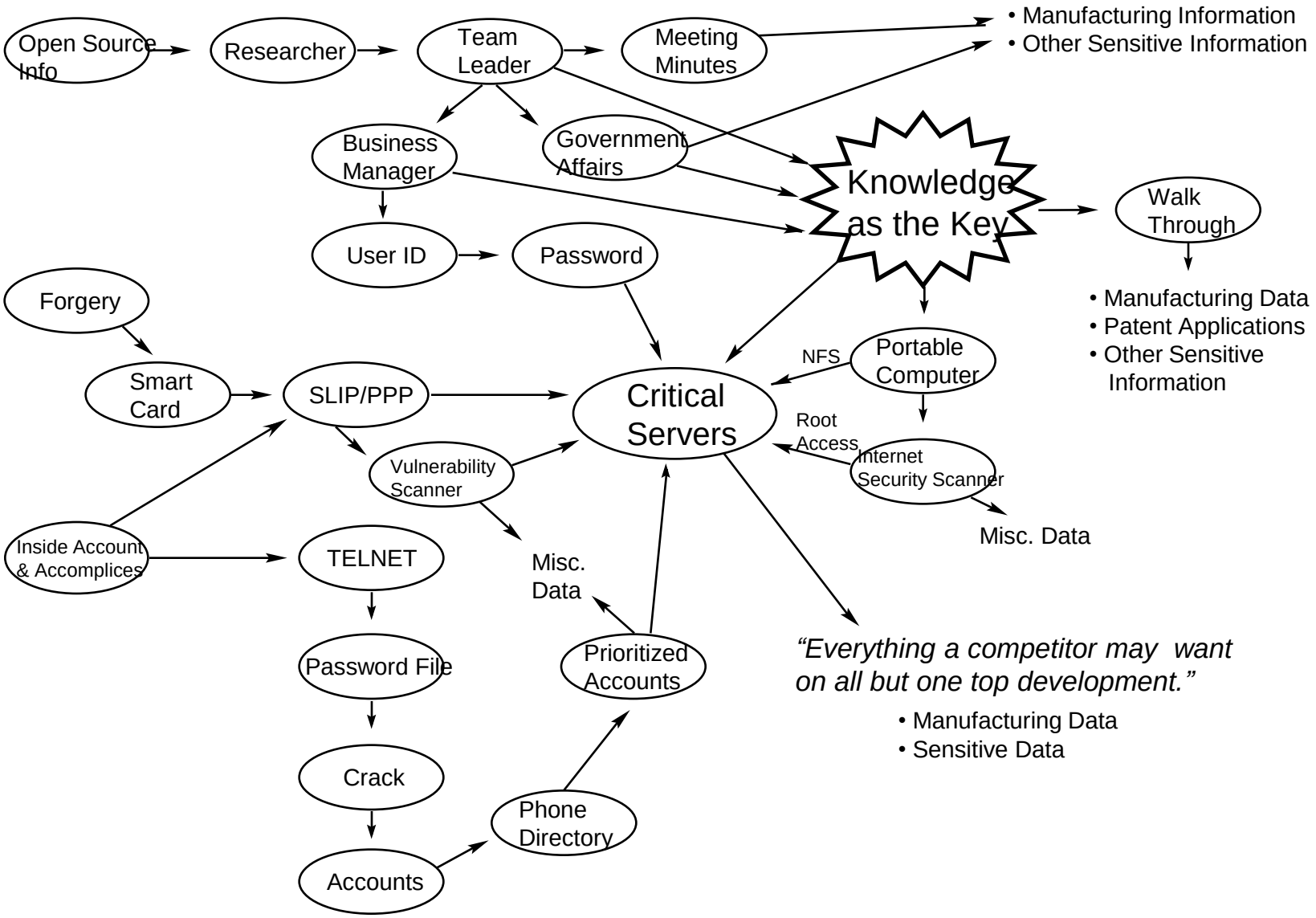
http://www.linkedin.com/in/irawinkler

Case Study #2

- Placement of a person as a temporary employee in a high tech firm
- Full scale industrial espionage simulation
- No holds barred attack
- Multi-faceted attack
  - Open source research
  - Misrepresentation
  - Walk through facilities
  - Internal hacking
  - Internal coordination of external accomplices

Background

- Company has many emerging developments
- Developments valued in excess of $10 Billion by Wall Street analysts
- Company has experienced several cases of industrial espionage
- Research mentality of openness causes an operational security nightmare
- Security manager is very well aware of the threat
  - Secures what he can


Open Source Info
Researcher
Team Leader
Meeting Minutes
• Manufacturing Information
• Other Sensitive Information
Business Manager
Government Affairs
Knowledge as the Key
Walk Through
• Manufacturing Data
• Patent Applications
• Other Sensitive Information
User ID
Password
Forgery
Smart Card
SLIP/PPP
Critical Servers
NFS
Portable Computer
Root Access
Internet Security Scanner
Misc. Data
Vulnerability Scanner
Inside Account & Accomplices
TELNET
Misc. Data
Password File
Prioritized Accounts
"Everything a competitor may want on all but one top development."
• Manufacturing Data
• Sensitive Data
Crack
Phone Directory
Accounts

Results

- All but one emerging development was seriously compromised
- Information valued in the billions of dollars
- Pending litigation posture compromised
- Patent applications compromised
- What else is there to say