Security: Built-in or Bolt-on?

Bill Anderson, CISSP
Information Security Specialist
Interhack Corporation
http://web.interhack.com/

What do we do?

- Information Assurance
  - Risk Assessment (RA)
  - Independent Verification & Validation (IV&V)
  - Penetration Testing (Pen Test)
- Forensic Computing
  - Electronic Discovery
  - Forensic data analysis

“Security” - What is it?

Protection of assets from threats
- Integrity
- Availability
- Confidentiality – Privacy

Risk management
- Value of asset vs. cost of protection

Ability to do business

How does Identity theft work

Get ahold of personal information

Profit

- Use directly (CC info)
- Sell to organized crime
- Apply for credit (SSN, etc)

Who are the bad guys?

- Insiders – frequently overlooked
  - Greedy
  - Disgruntled
  - Bored
  - Laid-off
- Professional hackers
- Script kiddies

How do Bad Guys get data?

- Exploit (high-tech)
  - SQL injection
- Exploit (low-tech)
  - Steal a backup tape or disk
- Walk in the front door
- Social Engineering
- Dumpster Diving

Bad Guy Economy

Won't spend $100 to steal $100

Big value targets

Easy targets

Strong security strategy

Make bad guys “pay” too much to hit you

- Layered approach
- “synergistic”
- Each layer multiplies level of security

Typical Network Engineering Problem: Bolt-on

Web access to application

- Let everything in
- Get hacked via OS vulnerability
- Add firewall
- Get hacked via SQL injection vulnerability
- Add application proxy
- Get hacked via application logic error or insider

Built-in vs. Bolt-on

Top down	Bottom up
Host/App security	Perimeter security (Network security)
Layers of complementary controls	Fight fires
Zone-based security	Minimum necessary to comply with regulation-of-the-week
Prevent fires	
Verify regulatory compliance	
Future-proof	

Built-in vs. Bolt-in

- Holistic
- Protecting assets
  - Reputation
  - Brand/Image
  - Ability to do business
- Logging/Monitoring
  - as part of process
- Least privilege

- Auditors
- Regulators
- Post-breakin forensics
  - could have been avoided if proper logging/monitoring/ auditing had been in place
- Blame game

Skip to the “good” part!

Built-in

- Architecture review
- Internal testing
- IV&V
- Pen Test (last!)

Bolt-on

- Pen Test first
- Bolt-on fix

Example: Large company requesting Pen Test

What they should have had:

- Internal hosts patched
- Internal hosts only running necessary services
- Procedure/policy to verify
- Firewall as an extra layer of defense

What they had:

- Firewall protecting externally visible hosts
- 2 years behind on patches
- Unnecessary services
- Incorrect firewall rules
- False sense of security

Dumpster Diving!

Reasons:

- 200 page documents; shredders with small capacity
- Managers not verifying disposal

One day worth of trash:

- 400+ Name, SSN
- 40+ Medical Records
- 20+ Name, SSN, DOB, etc
- 5+ Tax Returns

How do you protect your assets?

$50k cash

- Armored car
- Guards

How do you protect your assets?

Customer's identity and/or financial information

- On a CD via package delivery service, unencrypted?
- Unencrypted email?
- Value = 50k * $1500+ & damaged reputation

Physical Security

Every employee should be trained to recognize and report suspicious activity, unrecognized visitors

ID badges should be actively checked by all employees

Often left to guards

Once inside, intruder can often move about freely

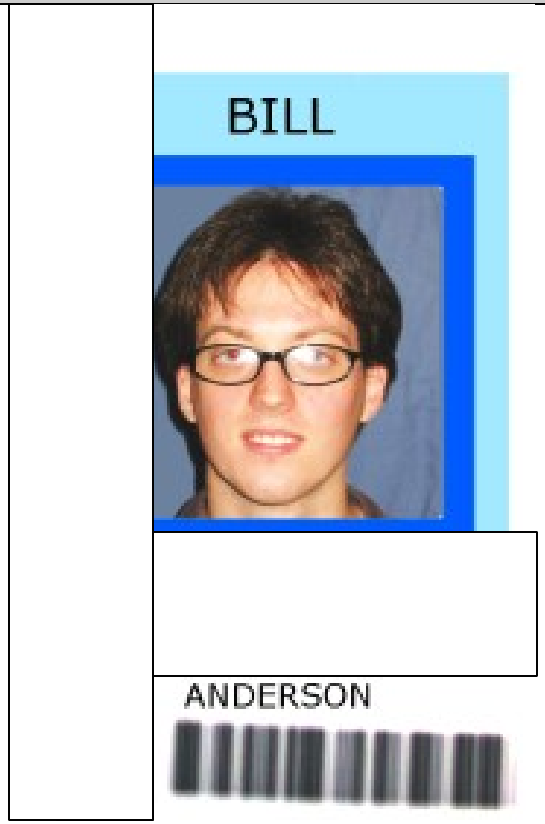
Wave to the camera

Example: Physical Security

High-rise office building

- 3-5 armed guards in lobby
- Multiple video cameras in lobby
- Video cameras on each floor
- Proximity card readers on each floor

Physical Security breakdowns



2 hours surveillance

$10 badge

- Fooled complacent guards

“Piggybacking”

- Employees too helpful, held door open for us

Questioned, but allowed to continue unreported

Social Engineering

Every employee should be trained regarding what information should be given to whom
Proper identity verification should be done for phone calls, etc.

What can't be found via network can often be found via social engineering

Excuses not to build-in

“We'll do security in version 2.0”
“Get it working, then we'll worry about security”
“It'll put the project over budget”
“We're too small”
“Nobody would want to break in to this”

Built-in vs. Bolt-on: Common misconceptions

Built-in

- Too much effort
  - Often requires more effort to re-engineer later
- Not my problem

Bolt-on

- "More convenient"
  - Only convenient until it fails
- "Cheaper"
  - Until it fails

Built-in: Accept responsibility, mitigate failures

- Build software defensively
- Plan to include patches and updates
- Availability
  - Load balancing, multiple sites, backups
- Integrity
  - SSL/TLS authentication, input validation
- Confidentiality/Privacy
  - SSL/TLS, data encryption, least privilege

Keys to Built-in success

Customers can be your most valuable assets
Value your customer's identity and financial information
Don't forget Brand and Reputation when considering the cost of failure
Don't just calculate cost to repair failure; be sure to include lost business, productivity, lost opportunities
Make sure all employees know that they are responsible

Work with Auditors and Regulators

- Your goal should be to protect your assets and protect your business, not just to get auditors and regulators off of your back
- Auditors should be verifying the work you've already done, not forcing you to do what you should have done

Who's responsible for security?

Everyone!
Data owners

That's what the “security team” is for!
Not my problem

Cost of failure

Lost sales
Regulatory fines
Litigation/Liability/Defense
Marketing – Repair image – if possible?

Value of success

Image built by good experience

How do you measure success in your organization?

Pen-Test - Verify how you respond

Disaster Recovery & Business Continuity Planning

Redundant design
Failover
Spare site
Off-site backups

Afterthought
Scramble

Example: Home computer

Real example

- Had AV, let subscription expire
- Has used anti-spyware scanners
- Occasionally used P2P networks to download music, etc.

Home computer; cont'd

Knock on door by State Police
All computers confiscated
Multiple felony charges
$$$ forensics expert, plus $$$ legal fees
Apparently victim of virus/backdoor acquired via P2P; found sharing illegal material
Less affluent person probably would have been forced to plea-bargain, lacking a forensic expert

Q&A?

This presentation is available at:

- http://web.interhack.com/news/n2005_billxln.php