



Data Protection Through Layered Security

Who am I

Brian Kirouac

Security Horizon

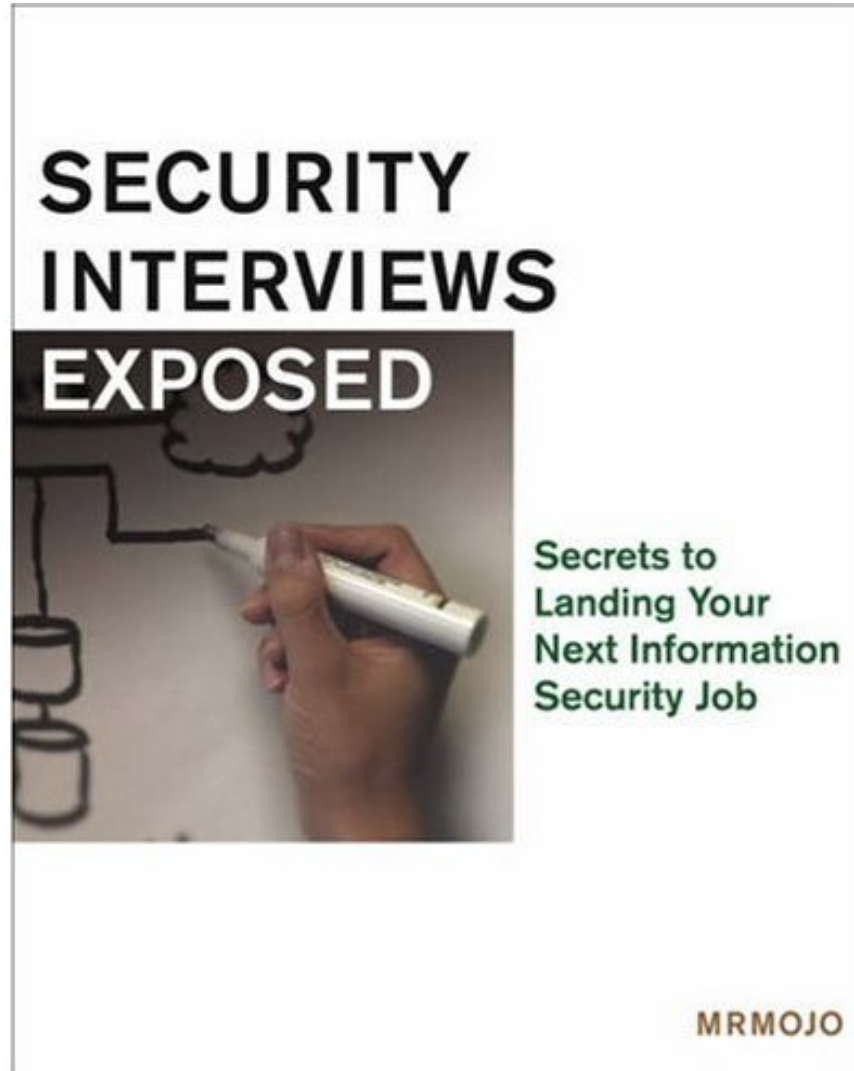
CTO, Principal

bkirouac@securityhorizon.com

I am a Geek



Upcoming Book



Security Horizon

- Small, Veteran Owned Business
- Founded in 2000
- Based in Colorado Springs
- Training
- Evaluations
- Wide Range of Security Experience
 - DOD, Government, Commercial

Why so many headlines?

- If we understand, why are there still so many horror stories in the news?
- Why are there still so many compromises?



- ✓ “Bank tape lost with data on 90,000 customers”
- ✓ “Dishonest executives face serious jail time”
- ✓ “Hacker pleads guilty in digital attack of eBay”
- ✓ “Santa Claus worm strikes in IM clients”
- ✓ “Hacker disables Kremlin TV”
- ✓ “Hackers steal \$50k from E-Trade account”
- ✓ “Students suspects of hacking into computer system”
- ✓ “IDs of 50,000 Bahamas resort guests stolen”

Did You Know?

- Based on some Federal documents you could potentially be held liable if your computer is used to attack another individual or organization?
 - Failure to adequately protect your system
 - Even if you never suffer an impact
 - Consider the Public Relations Nightmare
- You could be considered an “accomplice”

What *IS*
Security?

What Is Security?

- Security concerns the safety and well being of a particular entity.
- The dictionary defines security as:
se·cu·ri·ty (s -ky r -t) *n. Pl. Se·cu·ri·ties*
Freedom from risk or danger; Safety.
Freedom from doubt, anxiety, or fear;
Confidence
- In computer security, we are concerned with the safety of the data stored in the computer.

Common Security

- Door locks / keys
- ATM pin numbers
- Car Alarms
- ADT or Brinks Home Security
- Armed Guards
- Passwords
- Vaults / Safes
- Employees
- Video Cameras
- Porch Lights
- Pepper Spray
- ID Badges
- Caller ID
- Signatures
- Firewalls
- Parking Lot Flood Lights

Why Implement Security?

We implement a variety of security measures to protect something that is considered valuable.

- Jewels and money go in safes or vaults.**
- Homes have door locks and alarm systems**

What is
Information
Security?

What is Information Security?

- Information Security protects the data and information that resides in a computer.
- Ensures Authorization: Are you supposed to have access to the system?
- Access Control: What data are you allowed to access on this computer system?
- Ensures Availability: Can you access the data when required.
- Reinforces confidence in the integrity of data stored on the computer system.

What is Information Security?

- Information Security also deals with the integrity and privacy of data as it moves along the network.
 - Secure email transmission to avoid “eavesdropping” or “interception”.
 - Secure file transmission.
 - Secure network transactions; i.e. -
Purchasing merchandise on the Internet.

100% Effective Security!



100% Effective Security

There is currently no such thing as 100% effective security. Anyone promising this is bad news.

The idea is to balance the risk to your data with the cost of implementing protective measures.

Never spend more on security measures than the data itself is worth.

Common Security Problems

- Improper system configuration
- Ad hoc hardware implementations
- Security not focused around the organization's mission and critical information
- Security not integrated into the corporate culture
- Security not considered in the development process
- Lack of upper management support
- Lack of organizational education and awareness

Abstract:

- Technical solutions to security problems are incapable of addressing complete security.
- These solutions don't address critical information, business mission, standards and regulations, or the company culture
- They often result in wasted resources

The Problem:

- There is a perception that security can be solved solely through hardware and software
- Vendor products address particular problem areas within security
- Most organizations have not taken the time to identify their problem areas

The Problem - Products:

- Vendors want to sell product, that's how they stay in business
- Firewalls, Virtual Private Networks, Intrusion Detection Systems, Virus Protection, Technical Evaluation Services, Vulnerability Scanners

The Problem - Products

Product use must be customized for each organization based on their mission needs otherwise we're wasting valuable resources.

How useful are products?

- How do we know?
- What are we basing our opinion on?
- Products do not provide a complete solution on their own
 - Implementation without a complete picture leads to a failure of the entire security system

Lost Information

- Because products are not a complete solution, information can still leak through the system
- We don't have the appropriate focus
- Information is granular in nature and requires protection on multiple levels
 - We must understand all these levels

Products installed without
complete understanding
result in
inadequate security,
poor security posture,
and
wasted resources

Security Gap:

Security Objectives



Security Posture

What is My Risk?



Threats

Vulnerabilities

RISK

Asset Value
(Impact)



Can You Affect Your Impact?

- The Impact of a compromise is based on the value of your information
- The value of information can only be changed by changing your mission
- No real way to change this aspect of Risk



Common Threats

- **Password theft**
- **Vulnerabilities in public facing servers**
- **Unauthorized disclosure**
- **Brute force attacks**
- **Natural disasters**
- **Denial of service attacks**
- **Social engineering**
- **Malicious code**
- **Un-trusted individuals**
- **Identity theft**
- **Dumpster diving**

The Face of Hackers

- Hackers Have Grown Up
 - Most hackers want to make lots of \$\$\$
 - Hard to do that if you're in jail
 - Many are simply script kiddies
 - The really good ones already make lots of money and could care less about your network unless you're paying them to care
 - True hackers are simply problem solvers
- Your biggest threats are likely International, not Domestic

Who's Doing the Attacking?

- The Attacker Depends on the Target
 - Hostile Foreign Governments
 - Foreign Military
 - Competitive Businesses
 - Identity Thieves
 - Hobby Hackers (Crackers)
 - Professional Hackers
 - Users (Intentional or Inadvertent)



The Exception

- Virus Writers are the Exception to the Rule
 - The targets are unknown to the attacker
 - Attacker has a sense of anonymity
 - The true potential of a virus is never realized until it's too late
 - Successful (in most cases) due to lax configuration and patch management

Can You Change Your Threats?

- Organizations have very little control over the threats to themselves.

Affecting Vulnerabilities

- You have the most control over your vulnerabilities
- Reducing the number of vulnerabilities at your organization can reduce your RISK
 - It reduces the area of the Risk triangle
- Remember: Not all security vulnerabilities are purely technical in nature

The Right Direction

- Make yourself a less appetizing target
 - “I don’t have to outrun the bear. I just have to outrun the guy behind me!”
- Use appropriate tools
 - The hammer alone doesn’t build the house
- Work within your constraints
 - Smart decisions save resources
- Reinforce Management Buy-in!!!

Understand Real Examples

- You can learn a lot just by watching what is happening in the real world.
- Tons of the Fortune 500 have had security breaches of some sort.
- Consider the Public Relations nightmare resulting from the inadvertent release information that is covered by the privacy act or other regulations.
- If you understand what really happened, you'll be able to address customer concerns and questions about your own agency.

Good Security

- Depends on:
 - Smart Decisions
 - Management Buy-in
 - Knowledge
 - Experience
 - Qualitative and Quantitative Goals
 - Understanding what's really critical
 - Being able to objectively prioritize based on mission

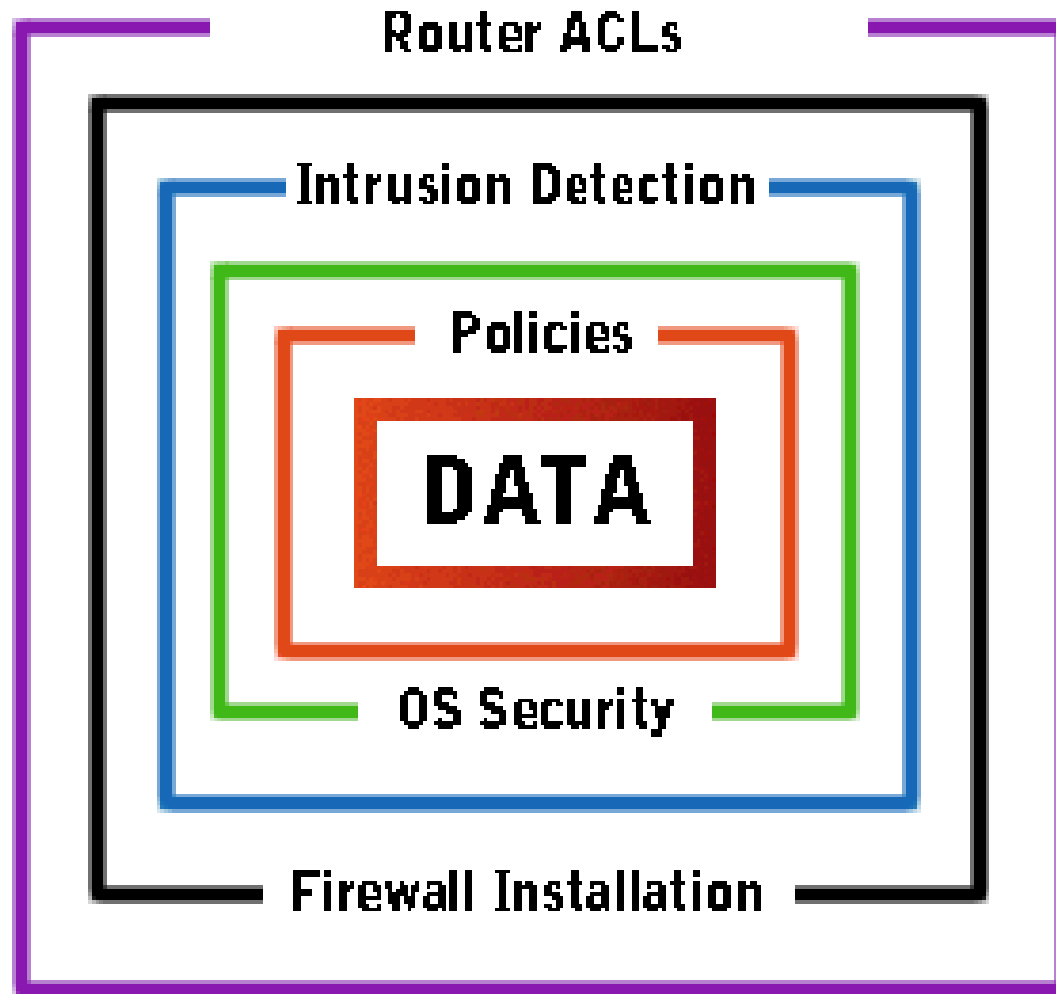
Use Layered Defense

- Create multiple layers of defense
 - Policies & Procedures
 - User Education
 - Secure Configuration (servers & workstations)
 - Network Perimeter
 - Router ACL
 - Firewalls
 - Auditing / Intrusion Detection

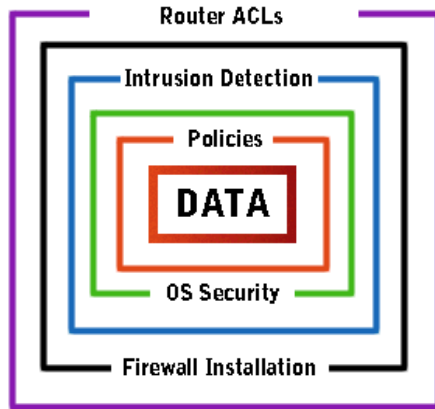
Aspects of Layered Security

- Management and Legal
- Technical

Layered Defense

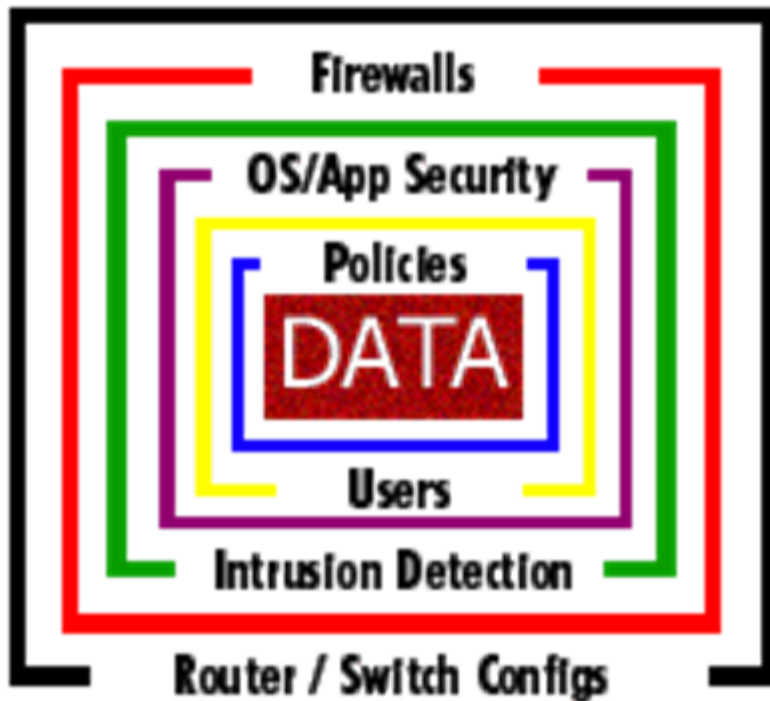


Layered Defense



- Security models help describe the various layers that help protect an agency's vital assets.
- You will decide how to implement.
- Other options fall into the various categories:
 - ✓ Virus software falls into the OS Security ring.
 - ✓ Security at the user level is in the Policies ring.
- The primary goal is protection of an agency's data.

What is Layered Security?



- Layered Security can be thought of as a castle with a moat, guards, drawbridge, etc.
- A firewall or IDS installation is not a total security solution by itself.
- True security exists on all levels.

Management and Legal

- Security Program Implementation
 - Security Policy
 - Security Procedures
 - Education and Training
 - Incident Response Policy
 - Incident Response Procedure
 - Due Diligence
 - Governing Law

Understand Your Information

- Critical information is based on your mission
- How critical is your information to your organization?
 - What happens if you lose:
 - Confidentiality
 - Integrity
 - Availability
- Consider the impact of these types of losses

Cultural

- Quality security depends on a culture of understanding
- Employees, customers, and management must understand the need for security
 - This may require education and training
- They must understand the consequences for failing to be secure

Cultural Change:

- Cultural change can not be addressed through security products
- They don't address Security Awareness Training or Understanding
- They don't address management "buy-in" for the security process

Organizational Policies

- Every organization needs direction, even for information security
- Create a quality policy that:
 - Outlines expectations
 - Sets Roles and Responsibilities
 - Provides Clear Guidance
- Market the policy internally
- Enforce the policy

Develop Security Policies

- Every quality security program starts with a security policy.
- Security policies provide workers with a focus and references for all agency security standards.
- Security policies will define what is and is not acceptable within the organization.
- They also define disaster recovery and incident response procedures.

User Policies



- Human element is generally your weakest link
- Function: Set of operating rules for people
- Security: Policies on password difficulty, data transfer, remote access, incident response, data sharing, etc.

User Policies



- Educate all users about computer and network security and security policies, as they relate to your agency.
- Users who are ignorant of the inherent risks of Internet access can often open up entirely new vulnerabilities.

100% Effective Security

- People are your last and BEST line of defense when it comes to information security.
- Security Awareness Training helps get personnel in the right frame of mind to protect agency assets, including information.
- Education is the key!

Train Your Users

- Not all users are security smart
- Many compromises occur because of user ignorance:
 - Unsafe configuration
 - Unsafe installation of software
 - Information Leakage
 - Insecure Operations

“Why should I lock my screen? There’s nothing of value on my computer.”

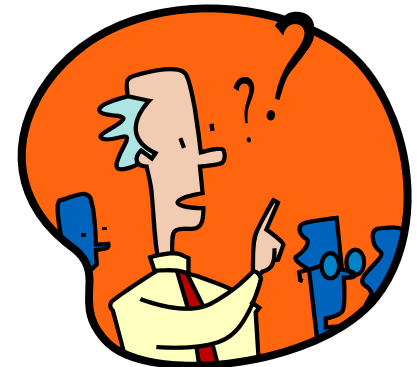
Educate the Workers

- **Security awareness training on an annual basis helps control the “out of sight / out of mind” problem.**
- **Employees not working in the security arena are not going to “think” security unless reminded to do so.**



Educate the Workers

- **Addresses important questions:**
 - **What is a threat? Virus? Hacker?**
 - **Why can't I use an easy password?**
 - **What do I have of value on my computer?**
 - **Why can't I write my password down?**



Operating Systems and Applications

- Function: Set of instructions the computer system operates under
- Security: Establishes/restricts acceptable protocols, services, users and processes. OS patches are critical.



Intrusion Detection



- Function: Passive monitoring of network traffic or sensitive hosts to detect unwanted activity
- Security: User defined ruleset, logging, connection dropping
- Functions as an “early warning system”

Firewalls

Function: Filters traffic by IP and service.

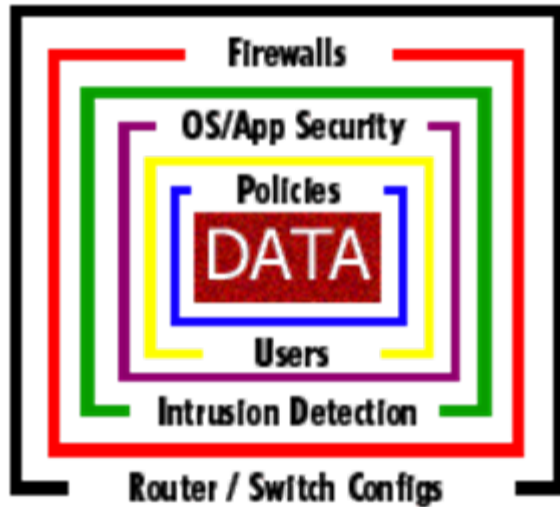
Security: Virtual Private Network (VPN), DMZ, controlled NAT, proxy services, authentication, and more.



Routers

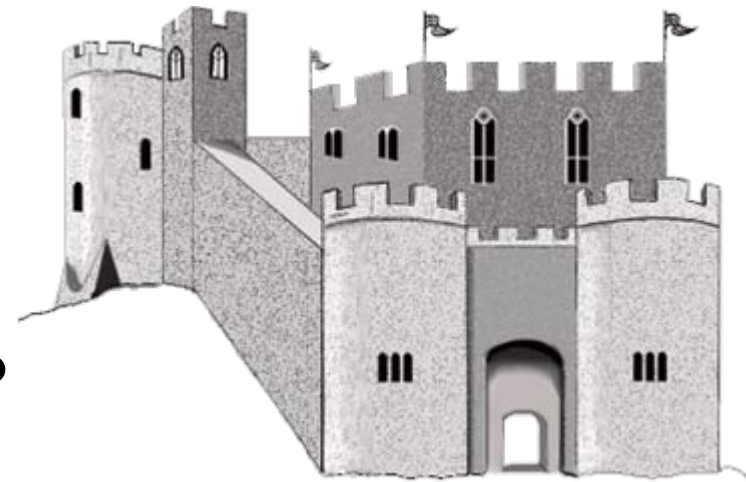
Function: Routes traffic to the appropriate network or subnet

Security: Filters IP addresses and services via the use of Access Control Lists (ACL)



Use the INFOSEC Lifecycle

- Starting with a Penetration Test is a waste of resources!
 - They're intended to test your security
 - If you've never been assessed or evaluated, how do you know what to secure?
- How difficult would it be to storm a castle if the drawbridge is down?



Use Security Specific Talent

- Hire a security professional or team to help guide you through your decision making and implement solutions.
- Network & System Administrators are hired to keep access open for workers.
- Security Administrators can help control access based on policies.
- Designating the network or system administrator as the individual in charge of security is a conflict of interest.
- Use the right tool for the job!





**SYSTEM/SECURITY
ADMINISTRATOR**
(And Chief Bottle Washer)

**SYSTEM
Things To Do**

**SECURITY
Things To Do**

\$250/hr Does NOT buy Quality

- Use your own internal resources to test consistently
- Use a third party firm with quality credentials to test annually
 - Big name firms may not be the best bet
 - Quality comes from experience, not cost
 - Check References

\$25/hr Does Not Mean Value

- Beware the fly by night company
- Final Reports that *look* like they came from Nessus, probably did
 - If it looks like a duck and quacks like a duck...
 - Many inexperienced firms lack the background to provide true analysis and reporting
 - “The Logo Shuffle” on the Final Report

Technical Evaluation

- Technical evaluations should occur from the highest priority systems to the lesser
- All systems are evaluated
- Mission critical systems are addressed first because they have the greatest impact on the organization
- Low priority does **NOT** imply lack of importance

Technical Evaluation

- Technical evaluations include vulnerability scans, port scans, application checks, host configuration checks, and manual probing
- Technical findings relate to problem areas that put critical information or systems at risk of compromise

Now Look at Products!

- The selection of security products should directly address the security findings
- Each product is different
- Each organization is different
- Product selection should be customized for the organization's needs
- This allows for a better security solution.

Now Look at Products!

- Pick the product that fits the problem
 - Firewalls are network based security
 - Virus protection protects against malicious code
 - Virtual Private Networks provide secure remote connections
 - File Integrity checkers provide Integrity for critical files or systems.

Buy it if You Need it

- Budgets are tight
- Don't buy something just because it's cool
- Purchases should be based on a need and can be traced back to policy goals

Recent News

Wednesday, February 7th 2007

Study notes link between IT sabotage, work behavior

http://security.itworld.com/4337/070207itsabotage/page_1.html

“Workers who sabotage corporate systems are almost always IT workers who exhibit specific negative office behavior according to recent research “

- Separation of Duties
- Change Control
- Host Based Intrusion Detection

Recent News

Monday, February 12th 2007

Veterans Affairs Notifying 1.8 Million People Their Data May Be Missing

<http://www.foxnews.com/story/0,2933,251600,00.html>

- External Hard Drive used for Backups
- Encrypt your backups
- Inventory control
- Proper label of data
- Proper controls on sensitive data

Recent News

Monday, February 12th 2007

Encrypted malware and code reusability

<http://isc.sans.org/diary.html?storyid=2223>

Well written malware, used certificates for encryption

- Restrict outbound traffic
- ACLs to limit certain type of internal traffic

Recent News

Monday, February 12th 2007

FBI loses laptops with classified information

<http://www.cnn.com/2007/US/02/12/fbi.laptops/index.html>

“The FBI lost at least 10 laptop computers containing classified information”

- Inventory Control
- Hard Drive encryption
- Laptop policy
- Data labeling
- Proper controls on classified information

Recent News

Monday, February 12th 2007

Another good reason to stop using telnet

<http://isc.sans.org/diary.html?storyid=2220>

Solaris telnet daemon allows login WITHOUT password

- ACLs to limit certain type of internal traffic
- Policy against telnet (and all non encrypted logins)

Resources

- www.iatrp.com – NSA IATRP Website
- www.securityhorizon.com – Security Horizon
- www.gssyndicate.org – Global Security Syndicate
- www.securityhorizon.com/security_journal/ - The Security Journal (online security periodical)
- www.nist.gov – National Institute of Standards and Technology
- isc.sans.org – SANS Internet Storm Center

Contact Security Horizon

- Call or email us today for more information:

Security Horizon, Inc.

5350 Tomah Drive, Suite 3500

Colorado Springs, CO 80918

719.488.4500

info@securityhorizon.com

www.securityhorizon.com



Mention this web demo and receive a 5% discount off of Security Horizon services!

Code: [cug0702](#)