Ethical Hacking—Part I

Understanding Your Risks

Ethical Hacking—Part I

What is the purpose of security?

- Think…

C

I

A

And, we do not mean a certain government agency in Langley, VA.

Ethical Hacking—Part I

What is the purpose of security? (Contd.)

- **The purpose of security is to insure the**

Confidentiality, Integrity, and Availability

of assets.

Note: Some sources also add 'authenticity' to the definition of security.

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

Security vs. Safety

- What is the difference between security and safety?
  - ***Safety*** is the prevention of adverse consequences from the ***unintentional*** actions of others or the random actions of nature.
  - ***Security*** is the prevention of adverse consequences from the ***intentional*** actions of others.
- Who is responsible for safety in your organization?
  - Historically, a 'safety office' was responsible for all aspects of safety. This approach was a failure because:
    - Safety was viewed as something to manage rather than something to prevent.
    - Incidents simply resulted in the safety office receiving blame, rather than the responsible party.
  - Today, the responsibility for safety is delegated throughout the organization.
    - Management usually sets policy and delegates implementation.
    - Implementation usually consists of:
      - Training all employees
      - Contingency planning and incident response
      - Monitoring, reporting, and regulatory compliance
    - In most organizations, ***safety is everyone's responsibility.***

Ethical Hacking—Part I

Security vs. Safety (Contd.)

- Who is responsible for security in your organization?
  - Most organizations lack a unified approach to security:
    - Physical security/access control
    - Industrial security
      - Intellectual property
      - Loss prevention
      - Transportation security
      - Telecommunications security
    - IT security
      - Computer security
      - Network security
  - Security is usually the responsibility of the cognizant organization.
  - Management usually delegates security policy to the cognizant organization.

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

Security vs. Safety (Contd.)

- Who is responsible for security in your organization? (Contd.)
  - What is wrong with this picture?
    - No unified management of security or setting of security policy
    - Security organizations have overlapping and/or conflicting responsibilities
    - Employee security training is usually lacking or incomplete
    - **Bottom line**: ***No one is really responsible for security!***
      Thus:
      - There are numerous convenient 'scapegoats' to blame when an incident occurs.
      - The organization continues to be vulnerable because there is no coordinated cohesive approach to remediating security problems.
  - What must be done to improve an organization's security?
    - Management must set security policy and delegate implementation to a single security organization.
    - Security must be implemented with the same approach as safety.
    - ***Security MUST be everyone's responsibility!***

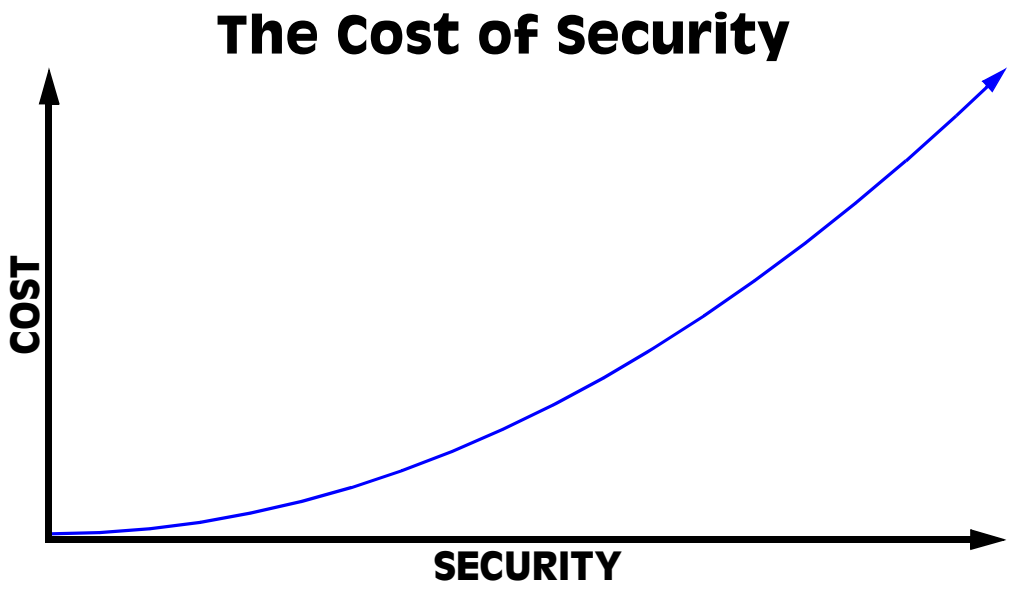
Ethical Hacking—Part I

What are the IT assets to be protected?

- Computers
  - Traditional computers: mainframes, servers, workstations, desktops, laptops, etc.
  - Industrial controls: SCADA, PLCs, EMS, BMS, security/access control, etc.
  - Personal devices: PDAs, cell phones, MP3 players, game players, etc.
  - Specialized devices: medical devices, cash registers, ATMs, etc.
- Networks
  - LANs, WANs, MANs, etc.
  - WLANs, WPANs, WWANs, WMANs, etc.
- Data
  - programs
  - information (and all forms of its representation, transmission, and storage)
  - knowledge ("peopleware")

Ethical Hacking—Part I

Security is not free.



Ethical Hacking—Part I

Security is not free (Contd.).

- From the graph, it is clear that:
  - Costs grow exponentially with increasing security[1]
  - Absolute security has infinite costs
- The objective is to maximize security at a reasonable cost.

  In other words, the objective is to minimize risk[2] at a reasonable cost.

The problem every organization must face is:

How much risk are we willing to accept?

Once that determination has been made, then the appropriate balance between risk and cost can be approximated.

1. ***security***: Freedom from risk or danger; safety. The level to which a program or device is safe from unauthorized use. Prevention of unauthorized use of a program or device.
2. ***risk***: The possibility of suffering harm or loss; danger. The probability of an undesirable event occurring.

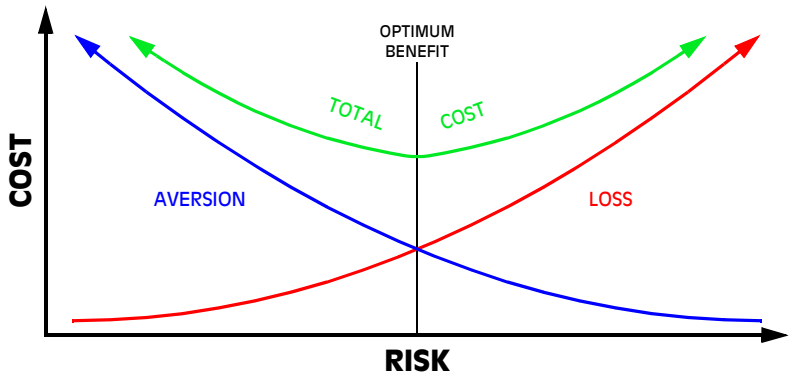
Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

Information Technology Security—A Risk Management Problem

- "The objective is to minimize risk at a reasonable cost."
  - This is essentially the definition of risk management.[1]
  - Effective risk management can minimize the cost of any identified risk.

Risk–Cost Optimization



1. ***risk management***: The process of making and implementing decisions that will minimize the adverse effects of loss on an organization.

Ethical Hacking—Part I

How do you assess IT security risk?

- Management approach:
  - How often is the event likely to occur?
  - What would be the cost of the loss?
  - LOSS / LIKELIHOOD = JUSTIFIABLE ANNUAL PROTECTION EXPENDITURE
- Technical approach:[1]
  - Popularity: How common is the attack?
  - Simplicity: How easy is the attack?
  - Impact: How substantial will be the loss?
  - Average of above 3 criteria gives a relative risk.

All approaches to security risk assessment are subjective!

1. Popularized by Foundstone, Inc.

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

Optimal security is *NOT* the objective!

- It would be *difficult* to state what is optimal security today, and *impossible* to state what would be optimal security tomorrow.
- Use security strategies that:
  - Work well enough,
  - Include hedges against various potential threats, and
  - Are adaptive.
- In other words, use *robust* security strategies!
- A robust security strategy:
  - Will probably not be near optimal under any circumstance;
  - Will perform well when compared with alternatives across a wide range of possible threats;
  - Will give satisfactory security against both easy-to-envision and hard-to-anticipate threats.

ROBUST SECURITY IS THE OBJECTIVE!

Ethical Hacking—Part I

How do you know if your security is effective?

- Technical evaluation:
  - If you do not detect any security breaches, does it mean that:
    - Your security is working but no one is attacking?
    - You are being attacked, but your security is failing to detect those attacks?
  - If you are detecting security breaches, does it mean that:
    - Actual attempts are being made to compromise your security?
    - Authorized accesses are being reported as attempted security compromises?
- Management evaluation:
  - Does the security work correctly?
  - Is the security worth the cost?

All approaches to evaluating security's effectiveness are subjective!

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

How do you know if your security is effective? (Contd.)

- The 5-step Approach to Evaluating Security's Effectiveness.[1]
  - What assets are you trying to protect?
  - What are the risks to those assets?
    - Who wants to attack it?
    - How might they attack it?
    - Why would they attack it?
    - What would be the consequences of a successful attack?
  - How well does the security solution mitigate those risks?
    - How well does it interact with everything it impacts?
    - What are its strengths and weaknesses?
    - How may it fail?
  - What other risks does the security solution cause?
    - What are the unintended consequences?
    - Would we be more secure without it?
  - What costs and trade–offs does the security solution impose?

1. Bruce Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World, Copernicus Books, 2003, pp. 14-15.

Ethical Hacking—Part I

Security requires a plan and policies to implement the plan

- Do you have a Security Risk Management Plan?
- Do you have written "Acceptable Use" Policies for your users?
- Do you have Configuration Management and Change Control Policies?
- Do you have a Physical Security Policy?
- Do you have a Data Security Policy?
- Do you have Software Development Policies and Standards?
- Do you have authority to enforce your policies?
- Do you have written Incident Response Plans?

These represent only a small sample of the security policies and plans that are essential for proper planning and management of an organization's IT security.

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

Security requires a plan and policies to implement the plan (Contd.)

- Do you have a plan, or is this how you respond to a security incident?

Ethical Hacking—Part I

What is the number one requirement for a good security administrator?

- A healthy dose of paranoia!

  If your hardware, software, users, and managers are not out to do you in, then all the miscreant hackers in the world surely are!

Ethical Hacking—Part I

Malware has become a serious security risk.

- What is malware?
  - Virus Hoaxes
  - Viruses
  - Worms
  - Adware
    - Web-based
    - Media Players
  - Spyware
    - Keystroke Loggers
    - Network Sniffers
    - Screen Capturers
  - Ransomware

Ethical Hacking—Part I

Malware has become a serious security risk (Contd.).

- What is malware? (Contd.)
  - Trojans
    - Application or System Programs
    - RATs
    - Web Sites
    - Users
    - Steganoware
  - Zombies
  - Bots and Bot Nets
  - Root Kits

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

Malware has become a serious security risk (Contd.).

- Most malware infections result from serious security lapses.
  - Users
    - Opening email attachments
    - Downloading files
    - Instant messaging/chat rooms
    - etc.
  - Administrators
    - Failure to patch systems
    - Failure to close ports
    - Failure to protect network shares
    - Failure to adequately protect VPNs
    - etc.
- According to U.S. DHS quoted reports:
  - Malware cost global businesses between $169 billion and $204 billion in 2004.
  - The average is between $281 and $340 worth of damage per machine.
  - Malware costs more than doubled between 2003 and 2004.

Ethical Hacking—Part I

What are your top technological risks?

- Unpatched operating systems and applications
- Improperly configured operating systems
  - Running unnecessary services
  - Excessive user or application privileges
  - Insecure permissions
  - etc.
- Systems that do not fail securely
  - Brittle: System becomes insecure on failure
  - Resilient: System remains secure, but potentially degraded, on failure
- Malware
- Insecure application programs, esp:
  - Browsers
  - E-mail clients
  - Groupware
  - Formsware

Ethical Hacking—Part I

What are your top technological risks? (Contd.)

- Poor programming practices
  - Operating systems
  - Applications and services
  - Database query
  - Web site forms and scripts

  that lead to vulnerabilities, such as:
  - Buffer Overflow
  - Cross-Site Scripting (XSS)
  - SQL Injection
- Clear text (not encrypted) data
  - Data storage
  - Data transmission
  - Authentication
  - Backups

Ethical Hacking—Part I

What are your top technological risks? (Contd.)

- DDoS Attacks
- VoIP
- SNMP
- VPNs
- Instant Messaging/Chat
- Open Content Web Sites
  (Blogs, Guest books, Wiki, etc.)
- Peer-to-Peer File Sharing
  (Kazaa, iMesh, eDonkey, Overnet, Grokster, Gnutella, LimeWire, G2, etc.)
- Wireless Access
- Physical Access
- Removable Storage Devices
  (Floppy Diskettes, USB Memory Sticks, MP3 Players, PDAs, Bluetooth Cell Phones, etc.)
- PBXes and Voice Mail

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

What are your top technological risks? (Contd.)

- Weak or no authentication
  - Passwords
    - User
    - Application (especially, embedded authentication)
    - Services
    - Default passwords:
      - Device management passwords
      - Software update/management passwords
  - Network protocols
    - Routing
    - NTP
    - DNS
- Backups
  - Unaudited backups
  - Off-site backups
    - Lack of adequate off-site backups
    - Insecure off-site backups

Ethical Hacking—Part I

What are your top technological risks? (Contd.)

- Security, Privacy, and Information Disclosure Threats:
  - Cookies & Pie
  - Flash
  - Digital Watermarks
  - MS Office Documents
  - Steganography
  - Cryptography
  - Spiders and Web Search Engines
  - Whatever is thrown away in the trash or resold
    (Paper documents, CDs, Old Hard Drives, Old Backup Media, etc.)
- Administrative and Privileged Account Logins:
  - Allowing direct login to privileged accounts
    - Use `runas` in Windows
    - Use `sudo`, `RBAC`, or `su` in Unix/Linux
  - Allowing users privilege on their local system
  - Allowing privileged accounts to access non-protected networks

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

What are your top technological risks? (Contd.)

- Inadequate accountability and auditability:
  - Baseline All Systems
  - Implement Universal IA[4]
    - Identification: Who Are You?
    - Authentication: Prove It.
      - Something you know (e.g., password)
      - Something you have (e.g., key)
      - Something you are (e.g., fingerprint)
    - Authorization: What You Are Allowed To Do.
    - Accounting: What You Did.
    - Audit: Did You Follow The Rules?
  - Have Strong Information Management Controls
    - All data must have a clearly identified owner.
      - IT ***never*** owns any data, except for system management and history data.
      - All data is owned by the business unit(s) that use it.
    - All data must be appropriately classified as to importance and confidentiality.
    - All data must have a clearly defined life cycle.

Ethical Hacking—Part I

What are your top technological risks? (Contd.)

- Inadequate understanding of asset criticality and failure risk:
  - Need to classify all assets by criticality:
    - **Safety Critical**

      Anything whose failure could result in an accident causing injury or death; or product, equipment, property, or environmental damage.
    - **Security Critical**

      Anything whose failure could result in the loss of the confidentiality, integrity, or availability of the protected asset(s).
    - **Mission Critical**

      Anything whose failure could prevent the production of product or delivery of service.
    - **Support**

      Anything whose failure could impact the operation of the parts of the organization not directly involved in the production of product or delivery of service.
    - **Ancillary**

      Anything whose failure would result only in inconvenience or the loss of productivity.
  - Need to understand the risk posed by each system's failure.
  - Allocate security resources based upon criticality and risk.

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

What are your top managerial risks?

- Inadequate organization-wide security awareness
  - Failure to make security everyone's responsibility
  - Failure to identify and assess security risks
- Inadequate and/or unenforced security policies
- Inadequate and/or untested security procedures
- Inadequate and/or untested disaster recovery plans
- Inadequate business continuity planning
- Inadequate IT involvement in regulatory compliance
- Too much "security theater"
- Failure to fund security based upon risk

Ethical Hacking—Part I

What is your number one risk source?

- Not hackers (but that risk grows daily)
- Insiders!
  - Over 80% of all reported losses are due to insiders.[1]
  - The average reported insider loss is over $40 million.[2]
  - The CIA's Office of the National Counterintelligence Executive reports: [3]
    - U.S. companies lose over $300 billion[4] in additional sales each year due to information compromised by insiders working for foreign entities.
    - Foreign governments and affiliated organizations account for 40% to 70% of all industrial espionage against U.S. companies.
    - In 2004, over 100 foreign governments targeted U.S. companies for industrial espionage, especially theft of trade secrets.
      - A small number of countries with large intelligence organizations account for most industrial espionage.
      - The Internet has made it easier for small countries to conduct sophisticated industrial espionage against not only the U.S., but against all industrial nations.

1. U.S. Secret Service
2. FBI/Computer Security Institute 2003 Survey
3. http://www.ncix.gov
4. Figure for 2001, the last year that the CIA/NCIX offered a public estimate.

Ethical Hacking—Part I

What is your number one risk source? (Contd.)

- Insiders! (Contd.)
  - The Office of the National Counterintelligence Executive reports: (Contd.)
    - The countries[1] with the most active industrial espionage activities against U.S. companies are:
      - France
      - Israel
      - China
      - India
      - Japan
      - South Korea
      - Taiwan
      - Pakistan
    - Compromise of information systems and data are the most common means of industrial espionage. (Conferences and trade shows are the second most common means and business relationships are third.)

1. For 2000, the last year that specific countries were identified. Order revised based on other sources.

Ethical Hacking—Part I

Who is your worst enemy?

- Not your average user
- Maybe a mole…
- Senior management is probably your second worst enemy.
- But your worst enemy is clearly **your help desk!**
  - They are trained to be helpful.
    - Create accounts
    - Change passwords
    - Provide access hostnames or phone numbers
    - etc.
  - They often lack adequate security awareness training.
  - They usually lack the tools to adequately authenticate their clients.

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

Why has security become such a problem in recent years?

- The explosive growth of the Internet
- Large numbers of security ignorant users
- Very buggy, insecure operating systems with default installations set to maximum insecurity
- Broadband connections that are "always on," thus providing both easy targets and easy means of future attacks
- Insecure communication protocols not designed with security in mind
- The addition of 'raw sockets' to Microsoft Windows O/Ses
- Organized crime has found that computer 'abuse' is an easy, low risk, source of income.

Ethical Hacking—Part I

Security courses seem to pick on Microsoft. Why?

- Because they have a disproportionately high number of vulnerabilities.
- Because they have a disproportionately high number of insecure systems using their products.
- Because their products are often distributed, installed, and configured using default options that disable whatever security is designed into the product.
  - Windows XP (disabled firewall)
  - SQL Server (no administrator password)
  - IIS (asp scripts that allow remote command execution)
  - etc.

Ethical Hacking—Part I

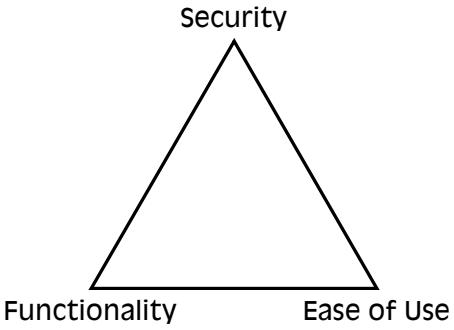
Why do Microsoft products have so many vulnerabilities?

- Relatively immature O/S:
  - MS-DOS predecessors: 1979
  - Early MS Windows: 1983
  - Windows for Workgroups: 1992
  - Windows NT: 1994
  - Compared to Unix:
    - First Unix Release: 1969
    - First Unix GUI (Smalltalk): 1974
    - TCP/IP Integration: 1982
    - First Public X-Windows Release: 1988
- Insecure design
  - Null sessions
  - Non-modular design (everything in kernel)
  - Critical system directories must be writable
  - Registry must be writable
  - Cannot isolate services into separate virtual environments
  - Exploitable O/S–process hiding functionality

Ethical Hacking—Part I

Why do Microsoft products have so many vulnerabilities? (Contd.)

- Because they have had an historical emphasis on functionality and ease of use at the expense of security.



Ethical Hacking—Part I

Why do Microsoft products have so many vulnerabilities? (Contd.)

- Inadequate testing leading to stability problems
  - Blue Screen of Death
- Non-adherence to standards
  - TCP/IP
  - LDAP
  - Kerberos
- Business practices
  - E^3
- Readily available hacking tools
  - NT Hacking Kit (a.k.a. NT Resource Kit)

Ethical Hacking—Part I

O/Ses are not the only problems.

- Other O/Ses have their share of weaknesses, too.
- Social Engineering
- Applications Software
- Electronic Surveillance
- Design weaknesses in every aspect of our IT systems
- Implementation flaws in every aspect of our IT systems
- etc.
- All give miscreants a way to compromise security.

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

IT security has become an integral part of regulatory compliance.

- Sarbanes-Oxley
- Gramm-Leach-Bliley
- Health Insurance Portability and Accountability Act
- FDA GxP
  - Good Academic Research Practices
  - Good Laboratory Practices
  - Good Clinical Practices
  - Good Manufacturing Practices
- NERC
  - Urgent Action Standard 1200
    - Critical Infrastructure Protection
    - Cyber Security
  - Draft CIP-002-x through CIP-009-x Cyber Security Standards (was: 1300)
- etc.

Almost every industry now faces regulatory compliance issues where information technology security is a critical aspect of the regulatory compliance requirements.

Ethical Hacking—Part I

Inadequate IT security has become a legal liability.

- If someone hacks your HR database and uses the information for identity theft, what is your liability?
- If someone hacks your customer database and steals credit card information, will the credit card company hold you partially responsible?
- If a competitor plants information stolen from another competitor's product development systems into your product development systems, how will you prove you did not steal the data?
- If someone hacks your computer and uses information stored on it (or, captured by a keystroke logger) to empty your retirement account, who bears the loss?
- If someone compromises several of your systems and plants DDoS zombies on them that are used to attack another organization, you may be found liable for failing to adequately secure your computer systems.
- If someone installs a pay-per-view child pornography web site on one of your computers, who in your organization will go to prison for possession and distribution of child pornography?

Ethical Hacking—Part I

What is the bottom line?

Seek robust security strategies!

Ethical Hacking—Part I

What is the bottom line? (Contd.)

- You must have written security plans, policies, and procedures.
  - Acceptable Use Policy (AUP)
    - Email Use (including attachments)
    - Download Use
    - Software Installation
    - Encryption
    - etc.
  - Physical Security Policy
  - Data Security Policy
  - Software Development Policies And Standards
  - Monitoring Policy
  - Incident Response Procedures
  - Disaster Recovery Procedures and Business Continuity Plans
  - Configuration Management and Change Control Plans
  - Security Risk Management Plans
  - Regulatory Compliance Plans and Procedures
  - etc.

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

What is the bottom line? (Contd.)

- Practice Defense in Depth (DiD).
- Enforce the Principle of Least Privilege (PoLP).
- Systems must fail securely.
- Restrict Physical Access.
- Use Strong Passwords and Good Password Policy.
- Baseline All Systems.
- Implement Universal IA^4.
- Have Strong Information Management Controls.
- Have Strong Social Engineering Defenses.

Ethical Hacking—Part I

What is the bottom line? (Contd.)

- Harden Systems, Networks, and Applications.
  - Encrypt Everything.
  - No Exposed Services on Protected Networks.
  - Do Not Trust Client Data.
  - Unknown Systems Must Be Considered Insecure.
    - DHCP Networked Systems
    - Wireless Networked Systems
  - Prevent Unnecessary Information Disclosure (e.g., DNS).
  - Practice Defensive Programming.

Advanced Systems Engineering Technology
New Horizons Sacramento Security Training

Ethical Hacking—Part I

What is the bottom line? (Contd.)

- Keep Current Backups.
  - Archives vs. Backups
  - On-site vs. Off-site
  - Audit Backups.
  - Encrypt Backups.
- Stay Current.
  - Patch, Patch, Patch!
  - Subscribe to Vendor Security Bulletins.
  - Subscribe to Security Discussion Groups.
- **Security is *Everyone's* Responsibility!**

Ethical Hacking—Part I

A concluding thought…

Over 99% of all organizations spend more money on coffee than IT security.

If you spend more on coffee than you do on security, you will be hacked.

And moreover, you deserve to be hacked.

– Richard Clarke, Special Advisor to every President from Nixon through Bush II.