



Data Connectors – January 30, 2008

How to Strengthen Your Incident Response Program: A Hands - On Approach

Peter Bybee, CISSP, CISA
President/CEO
Vigilant Management Services



Company Background

- Founded 1989 – 18 Years in Business
- IT Security Projects, Risk Assessments Since '94
- Certifications include CCSE, CISSP, GIAC, CISA
- **3 Business Areas**
 - Professional Services – Risk Assessment, Consulting
 - Security Product Solutions & Implementation Services – Best of Breed Product Solutions
 - Managed Security Services – Vigilant Management Services (Founded 2001 as a division of Network Vigilance)
 - 7x24 Intrusion Monitoring – Internal & External
 - Security Product Support & Maintenance – Firewalls, IDS, etc.
 - Compliance Management – Logs, Reporting, Vulnerability Mgmt, etc.

Presentation Objectives



1. Opening Scenario
2. Current Trends
3. Defining Your Information Security Incident Program
4. The 4 R's of Incident Response
5. Outsourcing Security

Opening Scenario

- You have just become a Security Manager, CISO, or Compliance Officer within a 2500 employee size company. The DBA who is a close personal friend, has reported a potential security breach that appears to have occurred 3 weeks ago. After doing some analysis, you discover a rootkit installed on a SQL database server that houses your customer database. The database was encrypted, and based on the firewall logs you're reasonably sure that the data was not compromised, but you can't tell for sure.
- What do you do?

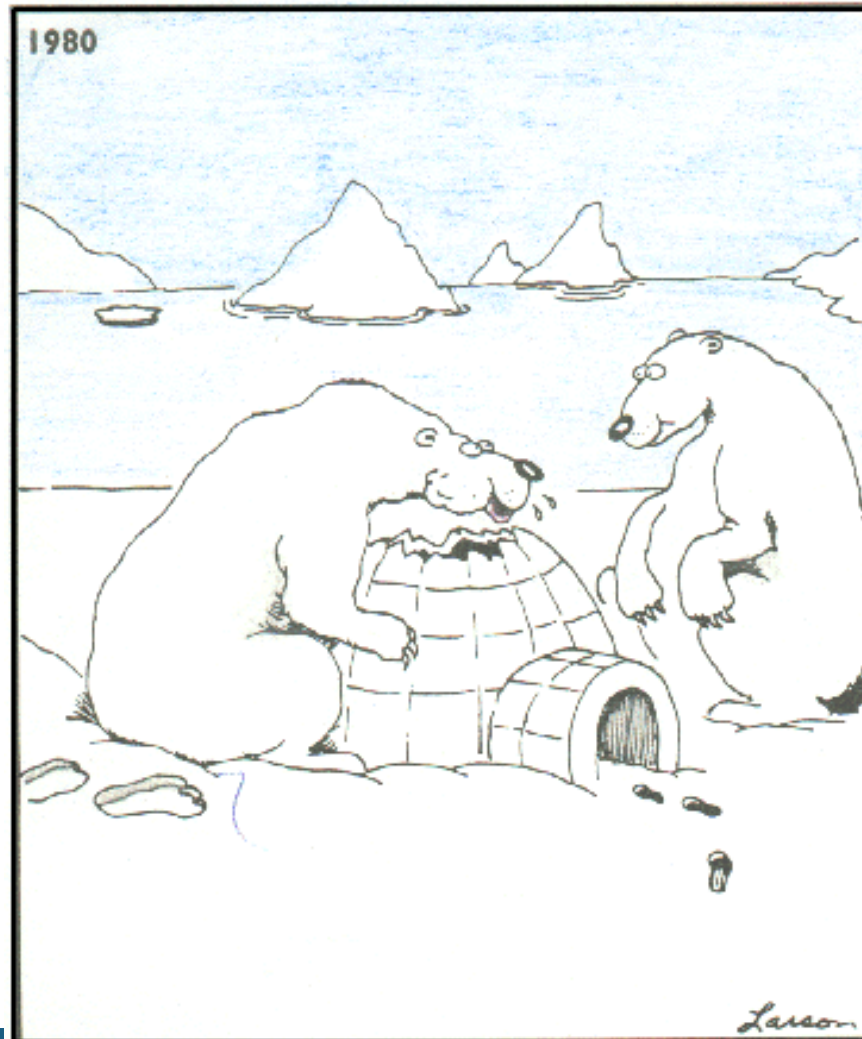
What do you Do?

- A. Initiate your incident response plan and notify law enforcement
- B. Inform Senior Management and take steps to send letters to all of your clients who may have had their data compromised
- C. Refer back to your last security assessment and see if anyone reviewed the security of the affected systems
- D. Do nothing and let the incident pass since you don't think you are affected
- E. Get your legal counsel involved to find a loophole somewhere so you don't have to disclose
- F. Find out how it happened, plug the hole/gap, and keep it under your hat within the IT Department.

3 Trends Currently That Are Exacerbating Risk

- Weakening/Fluid Perimeters
 - Multiple Entry Points
 - Wireless, VPN, Remote Desktop, RPC, etc.
 - Connections that bypass the firewalls & Security
 - How do you define the Perimeter in today's Network?
- Increasing Complexity of Networks & Applications
 - 1000's of exploitable vulnerabilities (MS had 97 Critical vulnerabilities released last year)
 - Shortage of qualified security staff, analysts, architects
- Increasing Sophistication of Attacks
 - Simple to Use & Automated attack tools
 - Designed for Large scale attacks
 - Attack sources hard to trace
 - Signature based virus/malware detection becoming less effective

Traditional Approach to Security



“Oh hey! I just love these things! ... Crunchy on the outside and a chewy center!”

The Nature of Vulnerabilities Have Not Changed



- Software with Bugs – Inadequately Patched or poorly Configured (worms, trojans, spyware, etc)
- Flawed Protocols & Weak Network Architectures (Allow for IG, MITM, Snooping, Hijacking)
- Carelessness & Human Curiosity (Social Engineering, viruses, IM, e-Mail, PW disclosure, Brute Force Attacks)
- Improper Physical Security Practices, Lack of proper inventory controls & Lax data destruction
- Backup/recovery & Application availability issues (DoS/DDoS Attacks)

Some of the Issues

- Insecure Protocols & Services
 - Telnet, ftp, snmp, SIP, etc.
- Known Default Settings
 - Passwords, snmp community strings, database logons
- System Design Errors
 - Access control errors, setup/configuration errors
- Software Implementation Flaws
 - Input validation, inadequate logic testing
- User Triggered Issues
 - E-Mail, Browser related, Social Engineered end-user tricks

1st Generation Threats

- Spreading mostly via email attachments, file sharing, bootleg software, Floppy disks
- Human Action Required
 - Execute an attachment like *.exe or *.vbs, or open a file embedded with a macro
- Single partite proliferation – code replicating
- Unsophisticated Stealth capabilities

Remedy: Discovery & Removal via AV

2nd Generation Threats

- Worms Leveraging Known Vulnerabilities
- Increasingly higher level of sophistication in replication strategy
 - Examples: Melissa Macro virus, Loveletter VBScript Worm (45 Million affected in 1 day)
- Viruses with multiple attack vectors
- Payloads both Destructive & Nondestructive

Remedy: Patching & Scanning

3rd Generation Threats

- Automated Attacks leveraging known & unknown vulnerabilities
- Collaboration of Social Engineering & Automated Attacks
- Motivation – Financially Directed, ID Theft, CC#, Phishing, pharming (DNS Cache Poisoning)
- Keyloggers, Trojans, Rootkits, & Bots (botnets)
- Signature Based malware (virus) detection is becoming less & less effective

- **Remedy: Proactive Security Enforcement, Network Access Control (NAC), Active End-Point Management, etc.**

● 2008 Threat/Risk Scenario

- The Professionalization of Computer Crime – Financially Motivated Attacks
 - Organized Crime Rings becoming a major force
- Firewalls and Anti-virus will increasingly become less effective because they are based on “known” attacks
- The Tide is shifting toward Stealthier Attacks
 - More difficult to detect
 - Extensive use of custom malware in “directed” attacks

Today's Topic

Not Today's Topic

- Vulnerability Mgmt Program
 - Proactive
 - Strategic
 - Seeks to Prevent Damage

Today's Topic

- CIR (Computer Incident Response)
 - Reactive
 - Tactical
 - Seeks to Minimize Damage

Before it Happens

You Need to be Prepared

First - Build an Information Security Program

- Owned by the organization's mgmt.
- Supported by policies
- Enforced by technologies
- Supported by a compliance program (training, awareness, etc.

Security Incident Response Program



- An Integral Part of the Information Security Program
- Owned by the Chief Security Officer
- Can be Implemented by IT Dept. (If managed In-House)
- Or you can Partner with a Managed Security Provider
- Addresses everyone: employees AND business partners
- Should utilize a phased, risk-based approach
- Formalized in a program with response team and supported by Security Incident and Response Policy and procedures
- Combination of In-house skills/capabilities and outside help
- Continuously measure, improve, and defend

- To Provide an appropriate level of safeguards (*internal controls*)
- To ensure the **Confidentiality Integrity Availability** of
 - data, information, networks, servers, applications,
 - related dependent technology services relying on the IT infrastructure and interfaces, that
- To help your organization **Identify, Contain Recover** Security Incidents.
- To better prepare for future incidents

Incident Response Policy

Key Elements:



1. **Objectives/purpose** of the Policy - prior slide
2. **Scope:** who must abide by the policy
All: employees and business partners
3. **Definition** of Security Incident vs. Events
4. **Explanation** of Incident types and prioritization by severity
5. **Ownership/mgmt.** commitment
6. **Roles and responsibilities**
 - Security Incident and Response Team
 - Authority/leadership
 - Identification, Reporting, Response, Metrics/Performance Measurement
 - Communication with law enforcement, media, and other outside parties
7. **Reporting** - How to report incidents/forms
8. **Procedures** to address various types of incidents

Security Event vs. Incident

- Event = observable occurrence
 - Firewall/IDS blocking of a service, dropping a connection, denying
 - E-mail gateway blocking 'infected' messages
 - Firewall Report showing blocked attacks
- Security incident = imminent threat, violation, or attempted violation of an organization's IT policy
 - Employee downloading database file with customer credit card numbers on a USB drive to work out of home or while on vacation
 - Contractor sending an unencrypted email with patient records to a 3rd party across the internet to troubleshoot an application system
 - Backup tape with customer bank account information is lost in transit
 - Attacker harvesting unprotected customer personal information on an unsecured web server
 - Attacker defaces website and requests \$1MM from the attacked company or else...
 - An action or inaction which exposes the company to legal liability based on the unauthorized disclosure of data

“At what point do you disconnect your entire company from the Internet during a quickly replicating computer incident?”

The 4 “R”s of Incident Response

● Readiness

- 65% of all efforts are spent here

● Recognition

● Response

● Recovery

Readiness

- Authority
 - Have a Documented Charter
 - Need Total Management Buy-In
- Roles & Responsibilities Defined
- Procedures
 - Steps to take, Decision Criteria, Escalation
 - Checklists
 - Note: This answers the Career Question
- Tools – Asset Mgmt, Collaboration
- Awareness Training, & Practice
 - Incident recognition, evidence collection
 - Planned Drills

Incident Recognition

● Evaluate Your Monitoring Sophistication

- Can you recognize an event? How do you Know?
- This is where a Managed Security Provider can really help you

● Recognition Tools

- Event Correlation, SIM/SEIM
- IDS, IPS, HoneyPots, AV alerts, network flows, etc.
- Outsource to MSSP? – Build vs Buy?

● Security Awareness Program

- Monitor User Complaints
- Users can detect anomalous behavior quicker than IT

Response: Roles and Responsibilities

- Security Incident and Response Teams:
 - Management Response Team: Who is in charge?
 - Technical Response Team: Who responds?
- CSO (Chief Security Officer)
- CIO (Chief Information Officer)
- Management – Who Liaisons with Executive Management
- User Community
 - Recognition of incidents and reporting
- Law Enforcement
 - FBI/InfraGuard, District Attorney (CATCH)
- Other outside parties:
 - Software vendors, Telecomm. Providers, ISP, Affected 3rd parties, Owners of attacking address, Incident Reporting Organizations, Media.

Security Incident Response Teams

Roles and responsibilities (cont)



- Management Response Team Members: Who is in charge?
 - Assigned one leader – Team Member Chair and Delegate
 - Members: CSO, CIO, IS mgmt, Audit, HR, Legal
 - Privacy Officer, Public Relations, and Physical Security (as necessary)
- Technical Response Team Members: Who responds?
 - Network and Voice Communications administrators
 - Server administrators - includes encryption key mgmt.
 - Desktop support
 - Developers – includes web developers
 - DBAs
 - Help desk, etc.

Can be comprised of employees or outsourced

Mgmt. Security Incident Response Team Roles and responsibilities (cont)



1. Provides authoritative risk-based mitigation action items to minimize impact
2. Confirms priority of incident types and communication by classification
3. Follows up to mitigate incidents and successful closure
4. Establishes and manages communication with outside parties
 - Includes law enforcement and Outside Parties to Obtain Assistance
5. Establishes and manages Data Disclosure process to affected parties
6. Manages training and education efforts for security incident awareness
7. Recommends to mgmt cost/benefit based investments for controls that enhance organizational resilience to incidents
 - People, processes, and technologies
8. Requests and utilizes metrics to measure performance and effectiveness of Security Incident Program
9. Assists mgmt, Legal, and HR in enforcing compliance with policies, procedures, and standards
10. Manages integration of Incident Response w/DRP capabilities for crisis mgmt.

Communication with Outside Parties



Incident Types and Prioritization

<u>Incident Prioritization</u>	<u>Incident Description</u>
Critical	High impact or potentially catastrophic impact on mission critical data assets
High-Priority	Moderate to High impact – may involve potential Violations of Company IT Policies
Medium-Priority	Moderate to Low Impact – Some loss/financial impact with regards to Integrity, Availability, Confidentiality
Low-Priority	Does not have a significant impact or loss with regards to Integrity, Availability, or Confidentiality

Incident Types and Prioritization

- Critical – Involves Systems Shown as DRP Priority Zero List or Impacting System Availability/Outages
 - **Denial of Service Attacks:** users unable to use mission-critical systems
 - **Unauthorized Data Disclosure:** Any type of incident resulting in unauthorized data disclosure to more than x records
 - e.g. Loss of unencrypted laptops, PCs, removable media with several thousand confidential records, etc.
 - **Disabling enterprise safeguards** (e.g..., firewall rules) that results in systems being unavailable or system data wiped out

- High-priority – Potential Violations of Company Usage Policies
 - **Unauthorized access:** Attacker running exploits to gain server root access and installs root kit detected by IDS and other safeguards
 - **Unauthorized access:** System admin accessing credit card data or intellectual property that could be used for financial gain
 - **Loss of unprotected assets with sensitive data** – under a few hundred records – still requires disclosure
 - **Inappropriate Usage:** Contractor uses another person's credentials on unattended workstation and performs unauthorized changes to a system

Incident Types and Prioritization (cont)

- Medium-Priority – Affects Data Integrity, Availability, Confidentiality, Some Loss:
 - **Inappropriate usage:** Sharing proprietary data with other 3rd parties
 - **Inappropriate usage:** Use of corporate assets to personal business
 - **Inappropriate usage:** Sending threatening emails
 - **Inappropriate usage:** disable safeguards (keycard access) in critical areas to facilitate 3rd party access
 - Maintenance by service provider or cleaning personnel results in unavailable (overheated equipment)

- Low-Priority - Affects Data Integrity, Availability, Confidentiality, No Loss
 - **Malicious Code:**
 - Workstations get infected viruses, worms, etc.
 - Remote PCs accessing network via VPN sending worm signatures
 - **Asset Loss/Theft:** Loss of passworded devices or encrypted laptops
 - **Inappropriate Usage:**
 - Emails w/ unpassworded sensitive data files, blocked by gateway
 - Use of another user's credentials on unattended workstation e.g....., sending email with inappropriate content to the company president

Risk Based Mitigation and Preparation

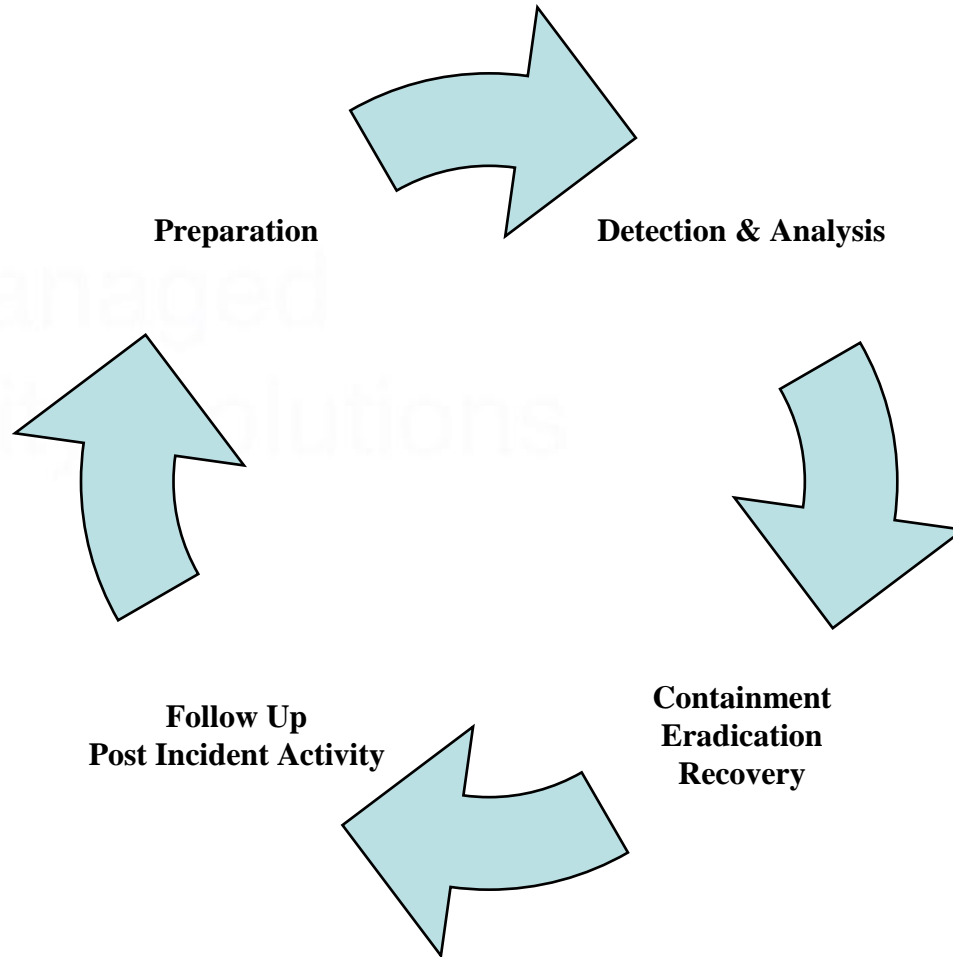
Preventive Controls (P)

1. Solid Patch Management program (P)
2. Critical Host/server and network security hardening (P)
3. Solid anti-virus/malicious code prevention
4. Regular vulnerability and penetration scans (P)
5. Maintain Accountability (P)
 - Inventory and asset tracking (P)
 - User Identity and Access Management (P)
 - Identify/inventory confidential data and control it (P)
6. User Training and Awareness (P)
7. Conduct Drills (P)
8. Identify existing skills in house and outsource (P)
 - Know when to ask for outside 3rd party Subject Matter Expert Assistance
 - Imaging and forensics

Detective Controls (D)

- Policy enforcement to test policy adherence (D)
- Logging and Monitoring (D)
- Forensic Software & Hardware devices

Incident Handling Process



Logging and Monitoring Policy and Process

- Administrative access
- File integrity checking (checksums, etc.)
- Honeypot logs
- Application access for sensitive transactions
- Time and date based – unusual access patterns
- Log correlation for all critical assets and safeguards
 - Monitoring, Analysis, Response Security
 - Firewalls, IDS, servers, network devices, etc.
- Syslog server centralized logging software
- Storage, Disposal, and Retention of Logs – example:
 - 30 to 60 days on syslog server
 - 60 to 90 days on tape
 - 90 days or older offsite
 - Destroy after 7 years per company retention policy

Security Incident Response Awareness Program



- Request mgmt to budget
 - Technologies
 - Staffing
- Require Confidentiality, Availability, and Integrity of data in job descriptions
- Confidentiality and Non-Disclosure Agreements resigned annually - job performance evaluations
- Mandatory online training quiz for all users – policy based
- Bring outside parties to educate sr. mgmt.
- Technical Incident Response Team
 - Continuing ed. w/expert knowledge e.g...., how to collect volatile data
 - Forensic certifications
 - Establish mentoring program
 - Testing of the Incident Response Program: Drills and simulations
- Build partnerships;
 - HR, Legal, Physical Security, Public Affairs/Media Relations, DRP
- Technology watch and information exchanges:
 - Local groups, law enforcement/InfraGuard, listservs, repositories w/advisory distributions

Incident Handling Must Haves



Current Contact Information Info	Cell phones, Pagers, Keys, email addresses for: Mgmt. Incident Response Team/Technical. Incident Response Team, Third Party
On-call information for unplanned downtime	All IS staff participating in unplanned downtime/ calling tree
Incident Reporting Mechanisms	Addresses on web site, Reporting Forms Calling the Help Desk
Partner Call List	Develop relationships with partners/vendors that can help assist you with forensics, investigation, etc, Have contracts in place beforehand
War Room/ and Secure storage area	Designated area for incident response coordination, area to store securely forensic evidence, etc.
Computer forensic software and workstations	Notebooks, evidence storage bags, blank encrypted USB devices, imaging software, spare workstations/ servers, digital cameras/audio recorders, portable printer, packet sniffers, protocol analyzers, CDs with trusted systems to gather evidence, other evidence gathering accessories and forensic software
Threat Information	Ensure that you have access to sources that can help you determine if the threat is localized, regional, or national in scope
Documentation	Baselines of trusted images of systems that need be rebuilt, cryptographic hashes, network diagrams, lists of critical assets.

What Can you Do?

Technology Checklist



- **Perimeter firewalls (with Reporting)**
- **Malicious code email filtering solution**
- **Web (internet content) filtering**
- **Intrusion detection and prevention (IDS)**
- **Log Collection/Log Management Software**
- **SIM/SEIM – Security Incident Management Software (event correlation)**
- **Patching – Processes, policies, systems**
- **EndPoint Security – Network Access Control**
- **Vulnerability Scanning Services – 3rd Party**
- **File integrity checking**

“Managed” Security

● Co-Management of Security Infrastructure

- Firewall Management
- Security Event Correlation/Detection
- Incident Response
- Forensics
- Reporting
- Real-time Intrusion Monitoring

● Business Benefits

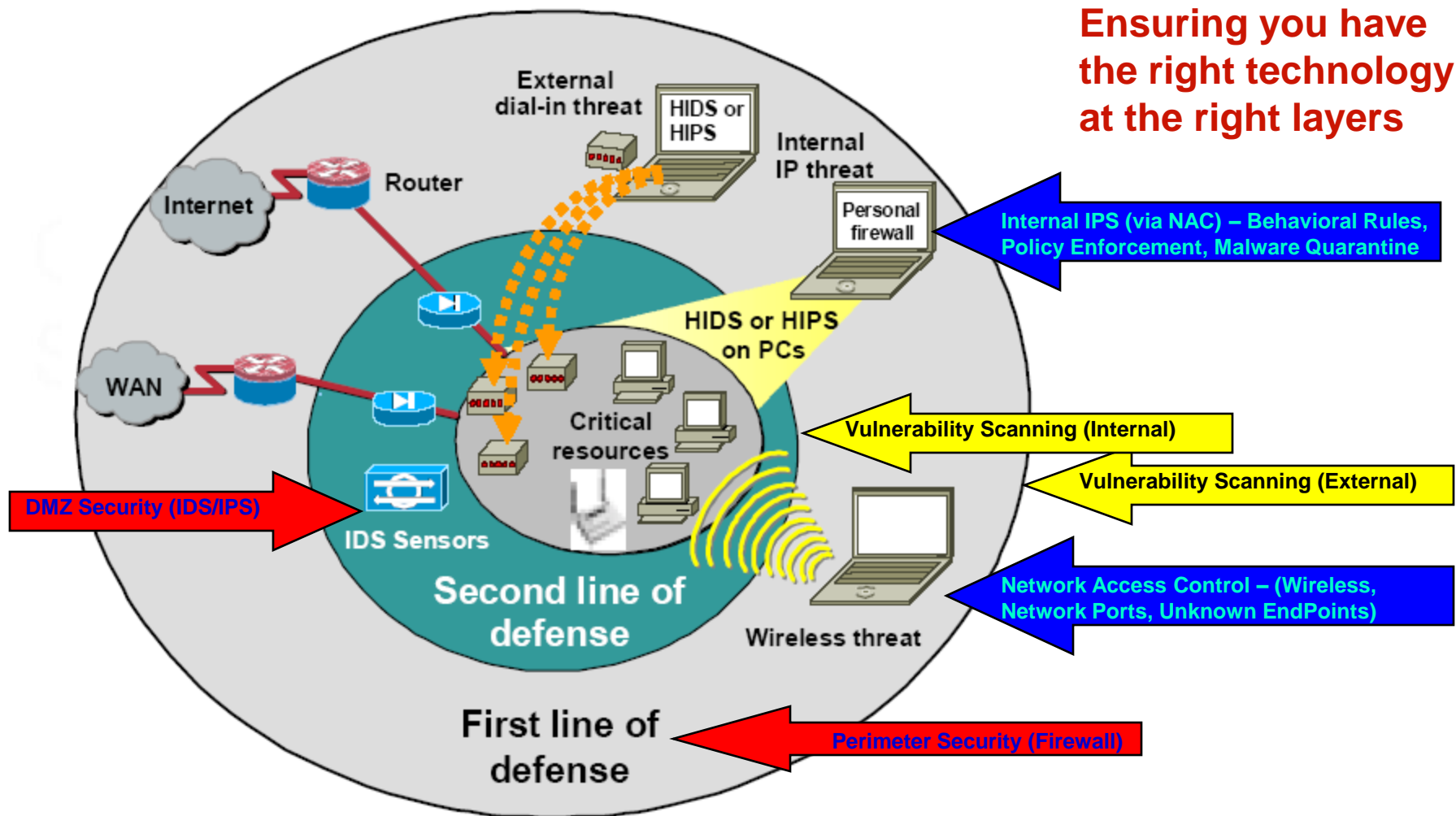
- Specialized Knowledge - Augment existing IT Dept Skills
- Fulfill Compliance Reporting Requirements (Sox, HIPAA, GLBA, PCI, etc.)
- 7/24 Monitoring & Alerting
- Automates critical manual & tedious tasks (security updates, patching, signatures, etc.)
- Cost Effective Alternative vs Staffing your own 7x24 NOC with multiple security skill sets

Using a “Managed” Security Provider



- Most organizations don't have the budget or operations expertise to manage
 - Technology - IPS, IDS, NAC, NBA Sensors,
 - Systems – Reporting, Help Desk, Event Correlation
 - Operations - Help Desk, Ticketing & Incident Tracking
 - Processes - Change Management, Best Practices
 - Personnel – Certified Intrusion Analysts, Experience
- It's not the total solution. You still have to take responsibility
- Using a Managed Security Provider Lowers the cost of Protecting Infrastructure
- It's not just about technology, it's also operations

Where does Managed Security Fit in your Multi-Layer Security Strategy?



Ensuring you have the right technology at the right layers

MSSP Selection Criteria

- Industry Expertise – Do they understand your business?
- Compliance Expertise – Do they understand your compliance environment/deliverables?
- Governance – Insurance (E&O, Liability), SAS-70 Certification, Incident Response, Financial Viability, Reference Checks, etc.
- Security Operations Expertise
- SLAs

MSSP SLAs

- Most are typically Weak & Lots of loopholes
In the past have come from Telcom carriers
- Availability/Help Desk SLA
- Intrusion Detection Response SLA
 - Events vs Incidents
 - Determination that an Incident has occurred
- If your Provider doesn't catch something, how will you know?

Making it Work with a Partner

- How are you Positioning the Provider's Service with your Internal IT Staff?
- Teaming up with your Service Provider
 - Making it Win/Win
 - Test Them, but tell them
 - Quarterly/Monthly Reviews

Conclusion:

10 Reasons Why Security Incident Response Program Needs to Be Constantly Updated



1. Temptation is too high: ID theft is the fastest growing non-violent criminal activity in the US.
2. Spending priorities in organizations may not focus on security.
3. Attacks are easy to conduct (9 yrs old and up).
4. Speed at which new attacks are created is high.
5. Hackers are creative and have a lot of time available.
6. Employees are curious and have spare time to 'poke' around.
7. Tools and technologies are not perfect.
8. It expensive to build perfect technology architecture with 100% risk coverage.
9. There is always a tradeoff between security and convenience.
10. People usually are the weakest link:
 - Process faults: Processes and standards sometimes do not exist, are bypassed, or carried out incorrectly.
 - Policy enforcement: 100% of policies cannot be enforced technically.

Assessing your level of Readiness

- Be prepared with an **incident response process** to:
 - Recognize
 - Respond
 - Contain
 - Mitigate
 - Learn from it!
 - Start building and audit it now
- **Test the incident response process** periodically because...
 - People, processes and technologies fail!
 - We are not in nuclear reactor or Defense Contracting industries.
- Bring in an **independent 3rd party to audit** the incident response process.
- Ensure your organization has **law enforcement contacts** (InfraGuard, local 'Catch Teams,' US Secret Service, etc.)

- **Database audit and controls: ISACA – Database Security and Audit**
http://www.isaca.org/Template.cfm?Section=IS_Audit_and_Control_Training_Week&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22705

- **NIST 800 documents:**
 - 800-61 Computer Security Incident Handling Guide
 - 800-86 Guide to Integrating Forensic Techniques into Incident Response
 - 800-92 Guide To Computer Security Log Management

- **CERIAS Center for Education and Research in information Assurance and Security Intrusion Detection Pages**
 - www.honeypots.org
 - www.Loganalysis.org
 - www.securityfocus.com
 - www.sans.org/rr
 - www.e-evidence.info
 - www.csrs.nist.gov
 - <http://icat.nist.gov>
 - www.cert.org/training
 - www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml

Q&A

For More Info:

Peter Bybee

pbybee@netvig.com

www.networkvigilance.com

858-695-8676

