Better Audits Through Improved Data Collection & Analysis

Paul Williams, MCSE, IAM, IEM
Chief Technology Officer
Gray Hat Research Corporation

ISACA Houston Chapter Meeting

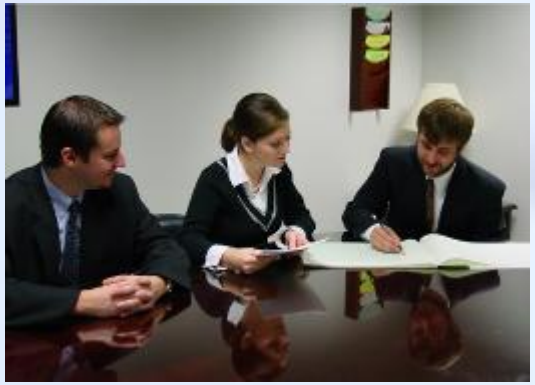
February 21, 2008

Presentation Overview

- Introduction & Company Background
- What Often Goes Wrong In A Standard Audit Approach?
- Examples: Negating/Bypassing Security Defenses
- How To Evaluate Technical Data Independent Of The Client's Explanations
- Understanding Basic Networking Technology Designs
- Evaluating Vulnerability Risk Exposure
- An Effective Technical Data Analysis Process
- Examples – "Thinking Strategically"
- Risk Assessment Process Output
- Questions & Answers

Commercial Security Consulting

- Extensive experience in strategic & tactical enterprise security:
  - Energy
  - Banking and Finance
  - National Critical Infrastructure
  - Medical Records
  - … and others

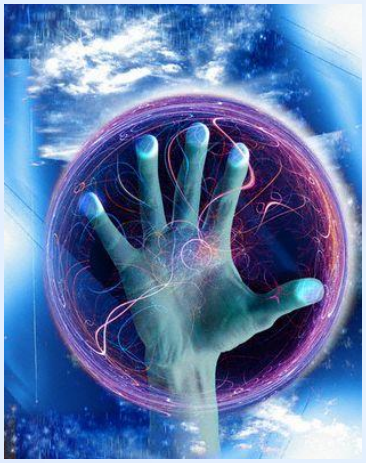


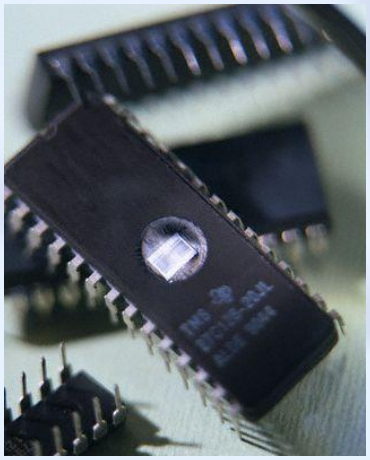
Government Security Consulting

- Extensive experience in strategic & tactical national security work:
  - Sensitive But Unclassified (SBU)
  - NATO SECRET
  - SECRET
  - TOP SECRET

Research & Development

- Cryptography
- Secure Communications
- Artificial Intelligence
- High Speed Databases
- Military/Defense Solutions
- Commercial Applications





Education & Training

Class Motto for our
Advanced Cyber Crimes Investigations
Course:

"No logs, no evidence, no suspects, and no obvious place to begin? NO PROBLEM!"

SPECIAL NOTE:

ONLINE HANDOUT VERSION CONTAINS A TRUNCATED OUTLINE OF THIS SESSION.

GRAY HAT RESEARCH CUSTOMER CASE HISTORY EXAMPLES AND PROPIETARY METHODOLOGY SLIDES HAVE NOT BEEN INCLUDED.

What Often Goes Wrong In A Typical IT Audit Approach?

Answer: The Audit Process Is At The Mercy Of The Client

- A client may supply incomplete, misleading, conflicting, or inaccurate information, or may not know enough to volunteer the right information
- The effort to obtain missing data and resolve discrepancies may take days, weeks or even months
- Key stakeholder interviews may produce self-serving results, or incomplete, erroneous or misleading information
- Even when discrepancies appear “resolved”, it does not mean they actually are. Later findings may start the data discovery process again, dragging the audit out further
- In a worse case scenario, significant data input errors may escape detection, potentially negatively impacting the results.

No wonder the audit process is lengthy, time consuming and typically produces results tied to standards compliance, rather than to the requirements of genuine security.

Solutions:

Evaluate Technical Data Independent of the Client's Explanations

Effective Technical Data Collection & Analysis Techniques, Part 1 of 5:

1. Discard the notion of a checklist compliance “audit” up front
2. Thoroughly understand your client’s business first before starting your examination of the client’s technology
3. Throughout the assessment process, examine the broadest possible view of each data layer first in terms of the applicable dependant business processes
4. Examine each new technical data layer in context of the defenses or weaknesses of the previous layer
5. **Expect** discrepancies and incomplete data; resolve discrepancies and omissions before moving further
6. If you aren’t noticing a significant client technical data error/data omissions rate (10–30%), don’t assume your client’s input data is solid and complete. Rather, it means something is wrong in your data analysis and interpretation process. No customer provided data set is ever anywhere close to accurate or complete.

   If necessary, get help from co-workers and start the technical analysis process over again.

Effective Technology Collection & Analysis Considerations, Part 2 of 5:

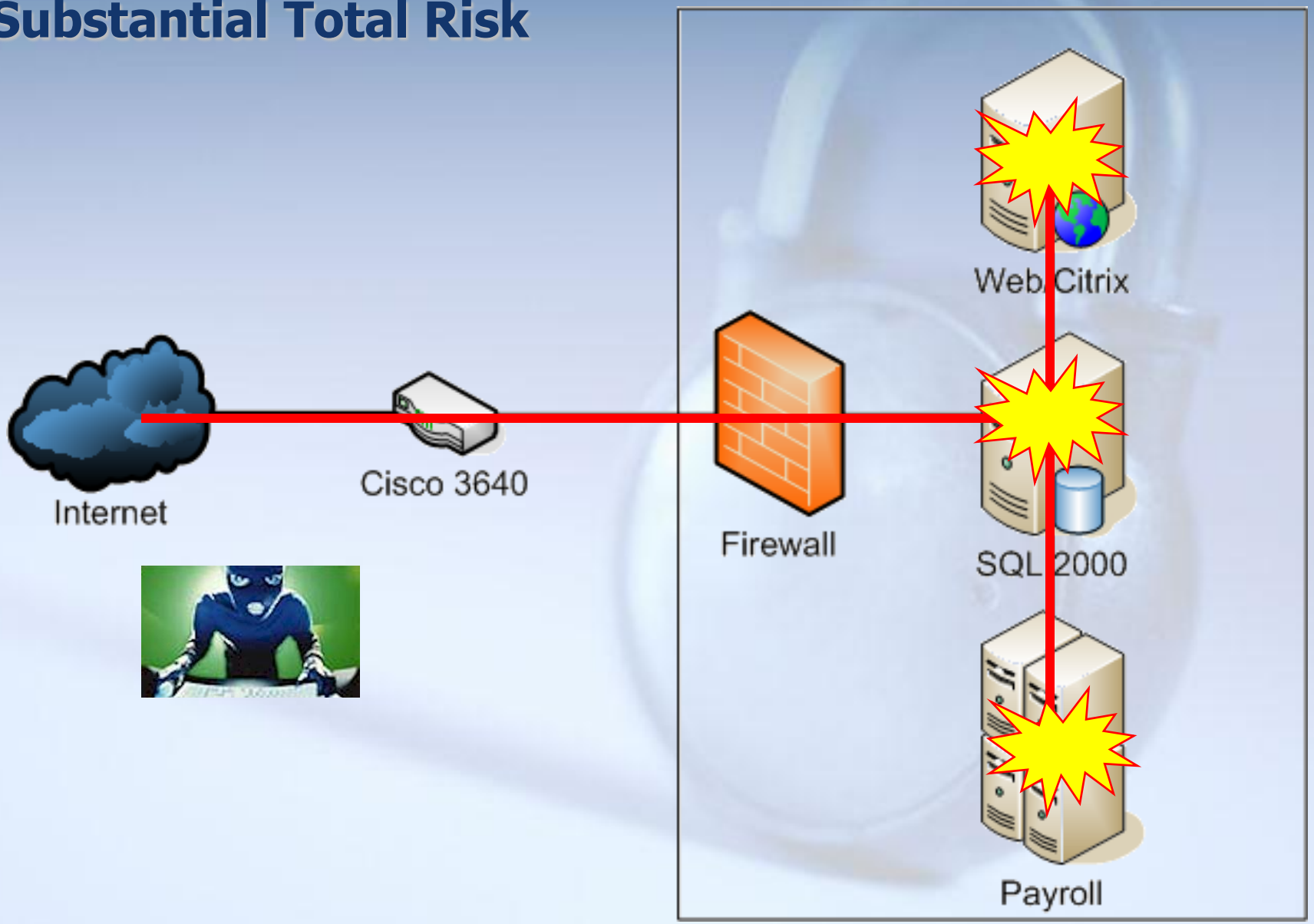
7. Start with the broadest possible interpretation of your client's network connectivity, starting from the outside and working in. This means starting with your client's upstream ISP(s) and working your way inwards through your client's perimeter defenses – including all client locations and any interconnected client or vendor locations, too
8. All routers and switches along the Internet connectivity path both to and associated with the perimeter defenses must be examined with equal intensity as the firewall(s), Intrusion Detection and Internet facing servers and applications
9. Determine what network traffic types are allowed and which are rejected, along with how and why
10. Keep in mind that the positive impact of each defense technology may be reduced, offset or bypassed by weaknesses elsewhere. In fact, this is the rule more than the exception. Make a specific point to look for such effects when examining each defensive precaution.

Technology Collection & Analysis Considerations, Part 3 of 5:

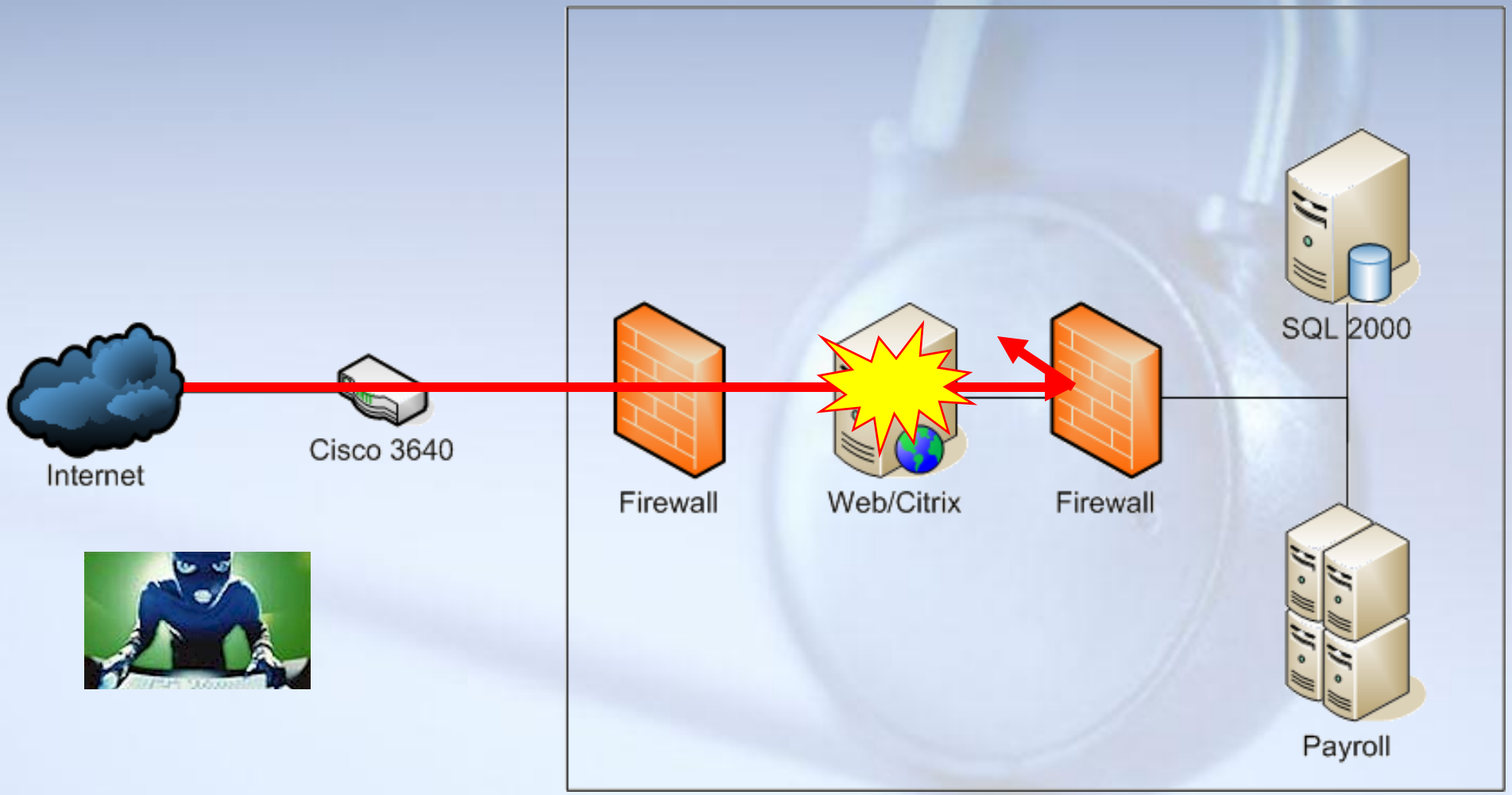
11. In your evaluation process, keep in mind that efficient and/or automated Auditing, Detection, Reporting, Case Tracking and Reaction capability can partially or largely offset the effects of other security weaknesses, although not entirely
12. When such systems are missing or inefficient, the impact of other security weaknesses should be weighted substantially greater in priority
13. Also consider the impact of *compartmentalization*: a network divided into zones to facilitate the natural containment of any breaches as well as allow prioritization of remediation efforts
14. Reduction of secondary vulnerability exposure can often be counted as high or higher as a reduction of primary vulnerability exposure.

Simple Networking Technology Examples follow next.

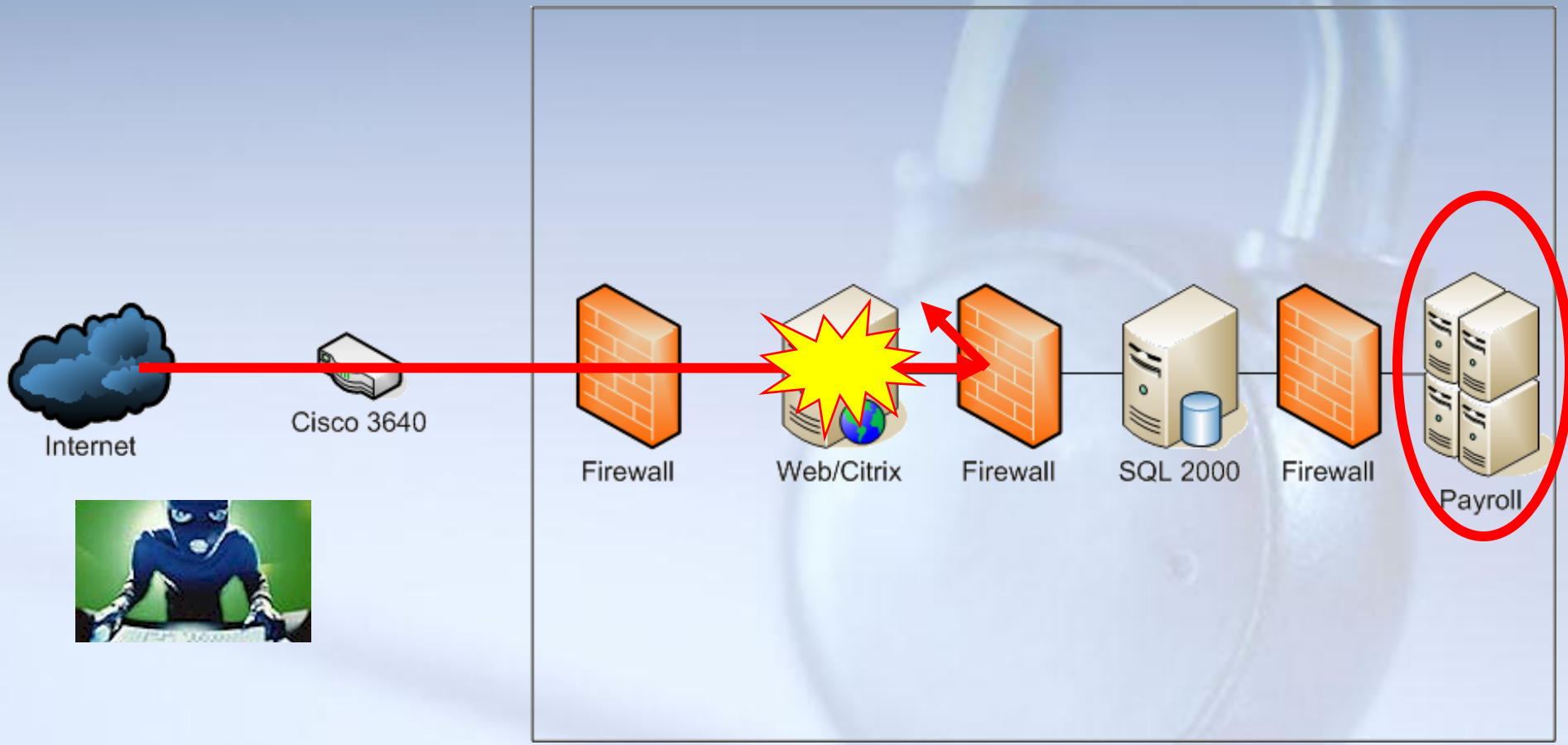
No Compartmentalization = Substantial Total Risk



Some Compartmentalization = Less Total Risk



Extensive Compartmentalization = Least Total Risk



Network design matters: Here the underlying equipment configuration remains the same, but is configured to present significantly less risk to this client's sensitive payroll information.

Technology Analysis Considerations, Part 4 of 5:

- Carefully consider multiple “What If” scenarios for each cyber defense: “What If” the primary defense fails? (examples to follow)
- Factor in the positive impact of effective secondary defenses by reducing the negative impact of primary defense vulnerabilities
- Factor in the negative impact of missing or ineffective secondary defenses by giving greater weight to primary defense vulnerabilities

More Networking Technology Design examples follow next.

Technology Analysis Considerations, Part 5 of 5:

15. Remember that hackers don't "play fair"
16. Any entry point into the network is equal fair game for hackers
17. Therefore all entry points into the network should be of equal assessment concern to you
18. Assess the risk from interconnected partner, supplier or customer networks; this can often be done indirectly without direct assess to those networks
19. When a high level risk assessment of an interconnected network is not possible, treat such interconnections as a threat similar to the Internet.

Examples Follow.

Technical Data Analysis Process Summary

- Once again, discard “checklist compliance” type thinking
- For your assessment report purposes, try not to think in terms of cyber security threats and vulnerabilities (attacks and defenses)
- Instead, think *risk management*
- While a risk management strategy resonates strongly with upper executives, its output is no better than the assessor’s understanding and analysis of the technology compromising the network
- Again, the best place to start your technical analysis is with your client’s network diagrams.

Want To Learn More?

Class Motto for our Advanced Cyber Crimes Investigations Course:

"No logs, no evidence, no suspects, and no obvious place to begin? NO PROBLEM!"

Next Class Date:

- **March 11 - 14: Montgomery College, Houston, Texas**

April 4, 2006 Volume 3, 4th Edition

Finding the Enemy Within:

Psychological Profiling Improves Protection Against Present and Future Insider Threats

by Paul Williams
Gray Hat Research President and Chief Technology Officer

The greatest threat to an organization's information assets is not found in the world of technology. A company's greatest liability is its people: the employees and personnel charged with making the business run.

Whether through negligence, carelessness, circumvention of policy, or deliberate th
assets, interr
risk exposure
physical solu
access can n

you
dentify
before
eed?
ew hire

Leave a Business Card or Sign up for our security newsletter at:

www.grayhatresearch.com

Questions ?

Gray Hat Research Corporation

Join our email list. Sign up at:
www.grayhatresearch.com

Or email: info@grayhatresearch.com

Thank You For Attending!

ISACA Houston Chapter Meeting