GTC

Risk Assessment, Scanning, and Security Planning

Ira Victor, GIAC G17799 GPCI GSEC
Director, Compliance Practice

Agenda

1. Who is your speaker?
2. Why security evaluations and planning is important [and what steps to take]
3. [Managing] The compliance process
4. Audit planning
5. Risk assessments
6. Vulnerability assessments

About Your Speaker

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

-> Information security consultant and auditor to corporations, law firms and government entities

-> Security certifications from the SANS Institute

-> Co-developer of patent-protected email security system

-> Board Member, Sierra Nevada InfraGard, a public private partnership between law enforcement and the private sector to protect critical infrastructure and stop cyber criminals. Represented InfraGard on SB410, NV Computer Forensics Bill

-> Member, Reno Lions. Provide security expertise for “computer for kids” program. Provides Lintel PCs to needy children

-> Director of Compliance Practice, Data Clone Labs

News Item: *Insider Threats Remain IT's Biggest Nightmare*

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

"A new study published by consultants Deloitte…finds that financial services companies -- among the most advanced and deep-pocketed consumers of security technologies in the world -- are still struggling with the concept of handling the insider threat issue despite all the cash they're dropping on security technologies.

In the survey of 100 global financial services firms, Deloitte found that *91 percent of those questioned were concerned about their inability to respond to insider threats*…"

PC World, September 22, 2007

News Item: *Latest FBI/CSI InfoSec Report*

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

-> Insiders are still biggest source of InfoSec incidents

-> Insider attacks now surpass virus attacks as the most common security incidents.

-> Nearly 60% of respondents have experienced insider-related events in the past 12 months, while only 52% report a virus incident

-> Each breach now costs an est. $350,454 to repair

Why is Evaluation and Planning Key?

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

1. Ever-growing IT Security regulations
2. More and more IT Security mandates
3. Increasing IT Security liability
4. Growth in demand for IT – data services, VoIP, mobile, wireless
5. Demands for managed change
6. Budget challenges
7. Other demands on your organization

10-Steps To Managing the Compliance Process

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

1. Look to internationally recognized standards and practices
2. Ex: ITIL, ITSM, ISO, CoBIT
3. Establish a working committee
4. Recruit key stake-holders
5. Draft a Charter
6. Have Charter approved by top management, the higher the better
7. Working committee develops plan
8. Approval and changes by top management of plan
9. Working committee executes and/or delegates plan
10. Working committee goes back to top management for reviews and input

Compliance

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

1. What regulations is the organization subject to?
2. What regulations are in the pipeline that could impact the organization in the near future?
3. How is the organization determining compliance, or lack thereof right now?
4. Where are the gaps in compliance?

Audit Planning

Audit Planning

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

1. Understand the scope of the audit

2. Prepare data flow diagrams and network diagrams and understand the difference between the two

3. Document business processes

4. Document all results

6. Participate in pre-Audit meetings with Auditor

Audit Planning, Phase II

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

GOAL – No Surprises

1. Assumption: you have already met with the auditor or representative BEFORE the audit
2. Have a team of INSIDE auditors BEFORE the audit – can be staff or consultants
3. Audit systems and procedures BEFORE the auditors show up
4. Document errors make corrections
5. Audit systems again
6. Remember, no surprises when the auditor show up

Audit Planning Example: PCI

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

1. Understand the scope of the audit
   -> Financial systems dealing with Credit Cards

2. Prepare data flow diagrams and network diagrams and understand the difference between the two
   -> Data flows of the *entire* CC process, network diagrams are narrower in focus

3. Document business processes
   -> Detailed processes people use in every step of the data flow

4. Test the same systems the auditor might test
   -> SSL tests, SQL injection tests, firewall tests

5. Document all results

Risk Management

“Risky” Terms To Know

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

1. Risk Management
2. Risk Assessment
3. Risk Analyses

What is Risk Management?

The optimal allocation of resources to arrive at a cost-effective investment in defensive measures within an organization. Risk management minimizes both risk and costs. -PCMag.com IT Encyclopedia

What Is Risk Assessment?

A report that shows assets, vulnerabilities, likelihood of damage, estimates of the costs of recovery, summaries of possible defensive measures and their costs and estimated probable savings from better protection.

-PCMag.com IT Encyclopedia

What is Risk Analysis?

A "risk analysis" is the process of arriving at a risk assessment, which is also called a "threat and risk assessment." A "threat" is a harmful act such as the deployment of a virus or illegal network penetration. A "risk" is the expectation that a threat may succeed and the potential damage that can occur. -PCMag.com IT Encyclopedia

What is Risk Analysis – Another View

A systematic method for addressing the risk triplet as it relates to the performance of a complex system to understand likely outcomes, sensitivities, areas of importance, system interactions, and areas of uncertainty.

The risk triplet is the set of three questions that the NRC uses to define “risk”: (1) What can go wrong? (2) How likely is it? and (3) What are the consequences? NRC identifies important scenarios from such an assessment.

-United States Nuclear Regulatory Commission (NRC)

Tying It All Together

As part of good Risk Management, we use Risk Analysis to measure (assess) and reduce the risks to Information Assets.

Fortunately for us, there are a number of great tools we can use to analyze risk!

Two Types of Risk Analysis

Before we look at the tools, it's important to know the two different types of Risk Analysis:

1. Qualitative
2. Quantitative

Both types can prove useful!

Qualitative vs. Quantitative Risk Analysis

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Qualitative Analysis:

- Helps in the identification of vulnerabilities that might allow threats to become reality
- Uses procedures that do not require the measure of the dollar value of information assets.
- More widely used than Quantitative Analysis
- Typically more difficult to use

Quantitative Analysis:

- Think threats and vulnerabilities
- Identifies the specific circumstances that could cause a loss
- Focuses on the annual cost of a loss and an objective measure of the likelihood of a loss
- Can put risk into dollar measurements
- Typically easier to use, but narrow scope may underestimate risk

Quantitative Risk Analysis

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Example: 1000 High Capacity USB Drives Issued by Organization

Cost: On average, $50 per drive

Loss: On average, 25% are lost within one year

Data Value: On average, $10,000 per drive

Quantitative Risk Analysis

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Estimated Physical Loss: $12,500 each year

Estimated Data Loss: $2,500,000 each year

$2,512,500 in Estimate Loss In One Year

How does this compare with a Removable Media and Control solution?

Qualitative Risk Analysis

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Example: $0 Online Stock Trading with Zecco

Phishing scams, keyloggers, cross-site scripting attacks = THREATS

Empty your stock account, make trades in your name = THREATS

Account only password protected = VULNERABILITIES

→ What are the ways to lower the RISK and still get your retirement account to grow?

Downside of Qualitative Risk Analysis

1. Not based upon dollars and cents
2. Can produce errors, since by nature it's subjective
3. Can be challenged by others with embarrassing results
4. Lack of hard facts can lead to distortions

Qualitative Risk Analysis

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Alternate way to trade stocks:

Walk into a stock brokerage office, or call them on the phone

Set up account, give them money, give them orders

This is lower risk, right?

Identify The Sources of eData

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Ameritrade Holding Corp… said computer hackers stole e-mail addresses and contact information for as many as 6.3 million clients and flooded them with spam stock tips.

So, the real risk may be at point we don't immediately identify -- the brokerages overall security paradigm, not just their web site

-> We may need to use objective information in our risk analysis to get an accurate picture!

Many Types of Risk Analysis Tools

Examples:

1. Fault Tree Analysis
2. Time Based Analysis
3. Failure Mode, Effects and Criticality Analysis
4. Monte Carlo Analysis

Fault Tree Analysis

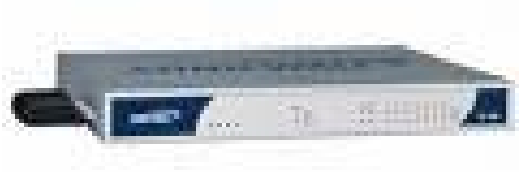
Developed by Bell Labs in the early 1960s

Logical diagrams are created to illustrate risks and potential failures

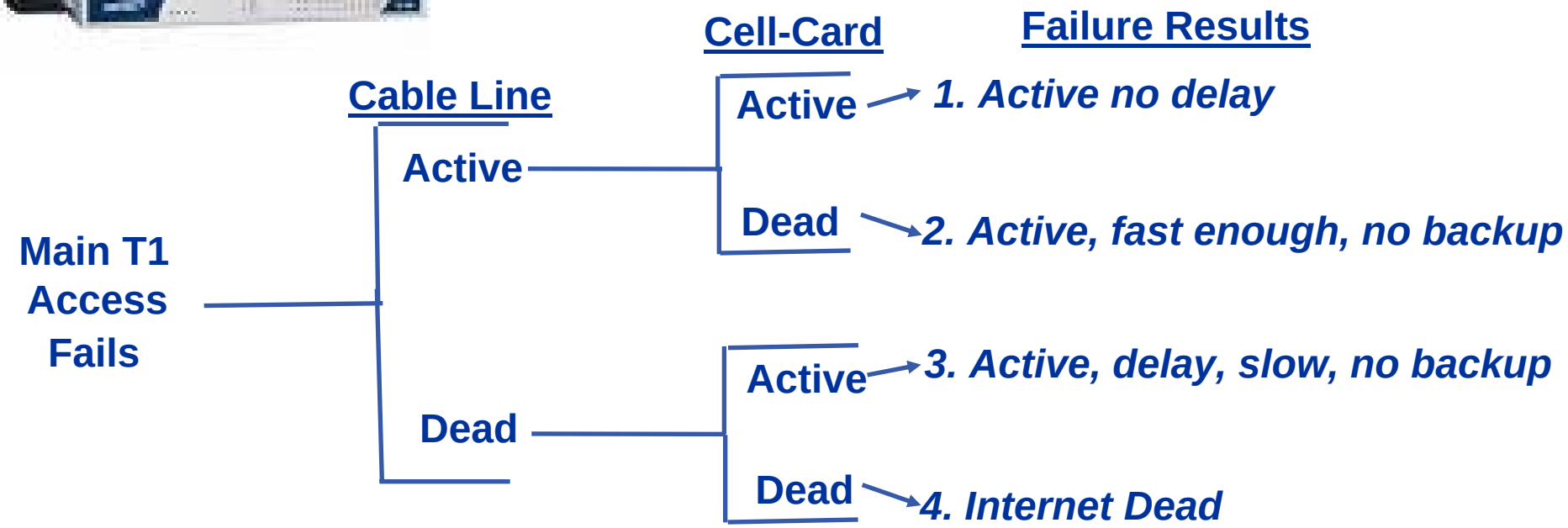
Undesirable events are first defined and a cause and effect relationships of the failures leading to the undesirable event are then identified.

Fault Tree Analysis Example

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com



← Firewall with Triple WAN – T1, Cable Modem, and 3g Cell Card



Time Based Risk Analysis

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

The process involves analyzing a system and identifying:

1. Preventative controls
2. Detective controls
3. Reactive controls

- Excellent in preparing for a failure before it occurs
- Measures the strength of exciting security measures
- Helps create procedures to use in the event of a failure or incident

Time Based Risk Analysis

The process involves analyzing a system and identifying:

1. Preventative controls = routers, firewalls, practices, procedures, and any other measure that protects a system from failures

2. Detective controls = logging alerts, IDS, separation of duties, and any other measure that indicates when a failure has occurred

3. Reactive controls = incident response teams, forensic investigators, and any other measure that comes to action after a failure has occurred

Failure Mode, Effects and Criticality Analysis

Identifies potential points of failure and classifies the failures according to severity values.

FMECA procedure

1. Define the system
2. Construct hierarchical diagrams
3. Identify potential failure modes
4. Assign impacts to the failure
5. Assign the severity
6. Rank failures in terms of severity and criticality
7. Produce reports highlighting major potential failures
8. Suggest strategies to reduce likelihood of a failures

Monte Carlo Risk Analysis Method

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Stochastic technique of Risk Analysis

Random numbers and probability statistics to measure risk

- Most complex
- Excellent at identifying seemingly unrelated risk terms are coupled
- Creates an overall picture of the range of possible results
- Can tell us the most conceivable outcome of a certain situation

Monte Carlo Example

~500 Students witnessed the shooting at Columbine

Different students report different number of shooters, number of people killed

Students can be asked and we can determine max and min numbers for each

We can create a chart for each respondent, and get a good idea of the numbers, and determine which outcomes are the most likely.

Vulnerability Assessment

Vulnerability Assessment

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

"Examination of an information system to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation." Institute for Telecommunication Sciences, a Division of the US Dept of Commerce

Vulnerability Assessments Tools

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

Two types of scans:

1. Outside looking IN = External Scanning
2. Inside looking IN = Internal Scanning

Two categories of scanners:

1. Open Source Tool - Ex: Nessus, Nmap, Nikto
2. Proprietary Tools - Ex: Qualys, GFI, ISS, many others

Hardware/software on the outside and/or inside of network

Some (like Qualys) also has web-based scanning tools for compliance for PCI external scanning only

Nessus

Nessus is a free and open source utility for vulnerability scanning

1. High speed discovery
2. Configuration auditing
3. Asset profiling
4. Sensitive data discovery
5. Vulnerability analysis of a network's security posture
6. Can be distributed throughout an entire enterprise, inside DMZs, and across physically separate networks

Windows and *nix versions are available for download

SEE: nessus.org and SourceForge.net

Nmap

Nmap ("Network Mapper") is a free and open source utility for network exploration or security auditing. Determines:

1. Hosts are available on the network
2. Services (application name and version) those hosts are offering
3. Operating systems (and OS versions)
4. What type of packet filters/firewalls are in use
5. Dozens of other interesting characteristics

Nmap runs on all major computer operating systems

SEE: insecure.org and SourceForge.net

Nikito

Nikto – free, open source web server scanner which performs tests against web servers

- Scans over 3300 potentially dangerous files/CGIs, and version specific problems on over 230 different types of web servers.
- Scan items and plugins are frequently updated and can be automatically updated (if desired).
- Not designed to be stealthy tool, test a web server in the shortest timespan possible, and it's fairly obvious in log files.
- Does a “house keeping” check for items that may not have a security flaw, but is helpful to know is security audits.

See: cirt.net and SourceForge.net

What VA Tools Can and Can't Do

Ira Victor GIAC GPCI G17799 GSEC
DataCloneLabs.com

CAN:
-> Help with audits
-> Help with penetration testing
-> Help with regulatory compliance
-> Key component in correction strategies

CAN'T
-> Eliminate the need for anti-virus or remove malware
-> Keep patches up-to-date
-> Backup your data
-> Detect a attacker that has penetrated your network
-> Eliminate the need for specialists to interpret actual vulnerabilities

VA Take Away

With so many options in the Vulnerability Assessment arena, don't be shy about talking downloading open source tools, talking to vendors.

Use the tools that work best for your needs at the time!

Re-cap

1. Who is your speaker?
2. Why security evaluations and planning is important
3. The compliance process
4. Audit planning
5. Risk assessments
6. Vulnerability assessments

Please fill out your evaluations!

GTC

Risk Assessment, Scanning, and Security Planning

Ira Victor, GIAC G17799 GPCI GSEC
Director, Compliance Practice