Integrity

SECURITY | RISK | COMPLIANCE

IT Risk Management

Because You Can Have Too Much Security

Introduction

- Fellow with Information Systems Security Association
- Certified Information Systems Security Professional (CISSP)
- President at Integrity, an information security, IT risk management and compliance consulting and services firm

Integrity

Overview

- What To Do….What To Do…
- Understand the Risk Equation
- IT Risk Management Cycle

Integrity

Scenario

Business: E-Commerce

Current Problems:

- SQL Injection vulnerability on public site
- Former system admin accounts not disabled
- Information security policy not updated in past 36 months

Where do you start?

Integrity

Scenario

You're implementing an MSSP SIEM solution. The vendor asks if you want to monitor end user devices (desktops, laptops, mobile, multi-function.)

What's your answer?

Integrity

Scenario

Most of your industry peers have “XYZ” technology implemented to solve a security risk. A vendor offers you an “end of month/quarter/year” deal that’s WAY below what you’d normally pay.

Do you cut the PO?

Integrity

The Correct Answer Is….

- ☐ Some of the above
- ☐ None of the above
- ☐ All of the above
- ☐ Would someone please give me the right answer so I can get back to sleep?

Integrity

Perspective

- Risk looks different for everyone
  - Internal
    - Executives/Owners
    - Everyone else
  - External
    - Customers
    - Board/Investors
    - Hackers

Integrity

Risk Management Approaches

- Structured
  - Proactive
  - Ensures risk is address appropriately
  - Can save money over time
- Knee Jerk
  - Completely reactionary
  - Often the true risk is not addresses
  - Never your best option

Integrity

Caution Ahead

- Customers, investors, citizens, politicians, regulators, competition, etc. will be extremely LOUD after an incident
- Decisions made with emotion rarely consider long term impacts
- Lack of time to plan causes decisions to be made hastily

Integrity

Example

A company was “hacked” after a virus was downloaded and they chose to rip out the Microsoft based network, replace it with a Mac network and covert their custom software from Cobol to Java.

Cost: $460,000

Integrity

A Better Approach

Hire a security consultant to identify the cause of the breach and recommend a course of action to include a network architecture change, upgraded anti-virus and ongoing monitoring.

Cost:$40,000

Integrity

Let's Define Risk

Risk = Asset x Vulnerability x Threat

- Asset
  - Resource that has value to the organization
- Vulnerability
  - Weakness of an asset which can be exploited
- Threat
  - Someone or something which will act on a vulnerability

Integrity

IT Risk Management

- Risk is rarely eliminated
- Typically no reward without risk
- Risk mitigation

Integrity

IT Risk Management Cycle

Integrity

Risk Assessment Criteria

- Asset Value (AV)
- Exposure Factor (EF)
- Single Loss Expectancy (SLE)
- Annualized Rate of Occurrence (ARO)
- Annualized Loss Expectancy (ALE)
- Control Gap (CG)
- Residual Risk (RR)

Integrity

Risk Assessment Methods

Quantitative

- Based on financial values
- Can be difficult to complete
- Rarely done without qualitative figures

Qualitative

- Not based on hard numbers
- Subjective
- Easier to accomplish

Integrity

Quantitative Example

Asset	Value	ALE (Fire)	CG	RR
Mainframe	$1.5MM	.088	.05	1.5MM(.038) = $57,000

An organization's mainframe asset worth $1.5MM has a threat of loss from fire with an ALE of .088.

The control gap that includes fire suppression lowers this ALE by .05 which leaves an ALE of .038.

An organization could expect to have a loss of $57,000 per year due to fire. Any additional risk mitigation techniques (insurance, fire detection/prevention devices, etc.) should cost less than $57,000.

Even techniques which are less than this may not be worth the money.

Integrity

Risk Management Options

- Implement Controls
- Transfer Risk
- Accept Risk
- Reject Risk

Integrity

Implement Controls

Administrative	• Policy and Procedures • Training and Awareness
Physical	• CCTV • Door Locks
Technical	• User IDs and Passwords • Firewalls • IDS/IPS

Integrity

Control Costs

- A control should not cost more than the expected loss
- Control Cost Considerations
  - Purchase Price
  - Implementation (consulting, training, downtime)
  - Maintenance and Operation (staffing, maintenance fees, replacement)
  - Operational Impact (performance, morale)

Integrity

Transfer Risk

- Assignment to a 3rd party
- Purchase Insurance
- Outsource

Integrity

Accept Risk

- Determine that the inherent or residual risk is acceptable
- Document risk acceptance by data owner

Integrity

Reject Risk

- Head…meet Sand…
- Not an acceptable solution
- Could constitute negligence

Integrity

Risk Left Unaddressed

Lots of time and money spent “fixing” the wrong problem.

When risk isn’t properly identified, you spend money to increase security without really increasing security.

Integrity

Summary

- It's all about managing risk
  - Evaluate, Calculate, Mitigate
- "An ounce of prevention is worth a pound of cure."
- Knee Jerk Security is Expensive!

Integrity

Question & Answer


dave.nelson@integritysrc.com


www.integritysrc.com/blog


DaveNelsonCISSP


@IntegrityCEO - @IntegritySRC


515-965-3756

Integrity