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
Overview

What To Do....What To Do...

Understand the Risk Equation

IT Risk Management Cycle
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?
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?
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?
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?
Perspective

• Risk looks different for everyone
  – Internal
    • Executives/Owners
    • Everyone else
  – External
    • Customers
    • Board/Investors
    • Hackers
Risk Management Approaches

• Structured
  – Proactive
  – Ensures risk is addressed appropriately
  – Can save money over time

• Knee Jerk
  – Completely reactionary
  – Often the true risk is not addressed
  – Never your best option
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
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
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
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
IT Risk Management

• Risk is rarely eliminated

• Typically no reward without risk

• Risk mitigation
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)
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
Quantitative Example

<table>
<thead>
<tr>
<th>Asset</th>
<th>Value</th>
<th>ALE (Fire)</th>
<th>CG</th>
<th>RR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mainframe</td>
<td>$1.5MM</td>
<td>.088</td>
<td>.05</td>
<td>1.5MM(.038) = $57,000</td>
</tr>
</tbody>
</table>

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.
Risk Management Options

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

Administrative
- Policy and Procedures
- Training and Awareness

Physical
- CCTV
- Door Locks

Technical
- User IDs and Passwords
- Firewalls
- IDS/IPS
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)
Transfer Risk

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

• Determine that the inherent or residual risk is acceptable

• Document risk acceptance by data owner
Reject Risk

- Head...meet Sand...

- Not an acceptable solution

- Could constitute negligence
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.
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!
Question & Answer

dave.nelson@integritysrc.com
www.integritysrc.com/blog
@IntegrityCEO - @IntegritySRC
515-965-3756