Is your Organization ready for a risk management program?

Bob Rudis • Liberty Mutual • @hrbrmstr
Lake Riskbegone

Where all the likelihoods are low, all the loss tables are populated & all the risk analysts are two standard deviations above the mean…
"Sir, the possibility of successfully navigating an asteroid field is approximately three thousand seven hundred and twenty to one!"
Objectives

- Analyze the gaps in your current organization
- Start framing even the most compliance-driven program in basic risk terms
- Gradually move from reactionary spend to qualitative/quantitative-based prioritization
<table>
<thead>
<tr>
<th>Security Policy</th>
<th>Asset Inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documented Controls</td>
<td>Business Involvement</td>
</tr>
<tr>
<td>Loss Estimates</td>
<td>Standard Definitions</td>
</tr>
<tr>
<td>Threat Profile</td>
<td>IRP</td>
</tr>
</tbody>
</table>
... is how an institution expresses its intent with regard to information security
Asset Inventory

...enables you to know what you have, where it is, who owns it, etc.
Documented Controls

...are specific activities performed by persons or systems designed to ensure that business objectives are met
Business Involvement

...ensures proper ownership & responsibility
Standard Definitions

...enables everyone to speak the same language
Incident Response Program

...ensures needed resources are identified & organized to effectively deal with adverse events
Threat Profile

...enables you to analyze, prioritize & communicate the most important threat actors/actions to stakeholders
Loss Estimates

... because you can’t have risk without the potential for loss
Metrics
"But, all we have are compliance controls!"
Ensure all risk statements in your control library are actual risk statements and not just descriptions of the control failure.
Require that individual control statements are specific to the application / device / system
- Loss of Confidentiality of PAN data in $SBU online payment system
- Loss of Integrity of Financial Reports in $SBU claims management system
- Loss of Availability of $SBU drug manufacturing monitoring system
Use a roll-up view when communicating your documented risks to management
Loss of Integrity of Financial Reports

Loss of Confidentiality of PAN data

Loss of Availability of Industrial Monitoring System
Take the offensive
http://www.sans.org/critical-security-controls/

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, & Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Device Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Security Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Loss Prevention
18. Incident Response Capability
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises
With the SANS Top 20 in hand, objectively enumerate your $ORGANIZATION capabilities and use this data to start a risk dialogue.
Audit Findings

Breach Response

Unsupported hardware/software
Consistent, calibrated & company-wide risk assessments
Demonstration that the risk assessments carry weight / affected change
Elevation of the risk assessment from a project management checkbox to critical path element when rolling out an app / network / system / etc.