Risk Management Approach to Cyber Insecurity
August 23, 2017
About Our Speaker

Baan Alsinawi
CISSP, CCSP, CRISC, CISM Certified

Founder and President, TalaTek LLC
Oakton, Virginia
Why Integrated Risk Management
Integrated Risk Management (IRM)

A set of practices and processes supported by a risk-aware culture and enabling technologies, that improve decision making and performance through an integrated view of how well an organization manages its unique set of risks

Source: Gartner.com IT Glossary
Why Integrated Risk Management?

- Regulations & Contracts Require It
- Due Diligence is Good Business
- SMBs are Cyber Targets
- Aligns Risk, Compliance & IT Security Operations
- Protect your Reputation
NIST Cyber Security Framework

Identify
- Asset Management (ID.AM)
- Business Environment (ID.BE)
- Governance (ID.GV)
- Risk Assessment (ID.RA)
- Risk Management Strategy (ID.RM)

Protect
- Access Control (PR.AC)
- Data Security (PR.DS)
- Information Protection Processes and Procedures (PR.IP)
- Maintenance (PR.MA)
- Protective Technology (PR.PT)

Detect
- Anomalies and Events (DE.AE)
- Security Continuous Monitoring (DE.CM)
- Detection Processes (DE.DP)

Respond
- Response Planning (RS.RP)
- Communications (RS.CO)
- Analysis (RS.AN)
- Mitigation (RS.MI)
- Improvements (RS.IM)

Recover
- Recovery Planning (RC.RP)
- Improvements (RC.IM)
- Communications (RC.CO)
IRM_ A Continuous Process

From the NIST Cybersecurity Framework
How to’s of IRM
Where to Start

- Defines the organization’s risk appetite
- Illustrates risks present for the business
- Make informed risk decisions
- Focuses investments
- Achieve compliance & security goals
Identify “Your” Risks

What constitutes an adverse event in your organization?

Do you handle medical data? Do you need to protect the privacy of the data?

Do your employees & contractors use laptops/work from home? Do you have a clear policy for handling company data? Stolen laptops?

Does your website need to be available 24/7? Do you have high availability infrastructure?

Do you outsource some of your business functions like HR or bookkeeping? How confident are you in their security & data handling practices?
Identify “Your” Risk Tolerance

What Constitutes a Low, Moderate or High Risk?

**Low**
- Website offline less than 12 hours
- Sales within 12 hours are $$ and you can tolerate that outage

**Moderate**
- Website out for 13-24 hours
- Sales projections impacted, we can still survive and recover

**High**
- Website out for more than 24 hours
- Sales significantly impacted, we may not survive
- Reputation impacted
### Identify Roles and Responsibilities

Who are the key stakeholders in your risk management program?

<table>
<thead>
<tr>
<th>Role</th>
<th>Role Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIO/COO</td>
<td>Responsible for ensuring there is are policies, tools, funding and resources to manage corporate laptops</td>
</tr>
<tr>
<td>IT Manager</td>
<td>Accountable for developing the procedures, selecting the tools and managing the resources</td>
</tr>
<tr>
<td>CFO/Finance</td>
<td>Consulted on the best way to implement the policy, what is practical, and cost efficient</td>
</tr>
<tr>
<td>Employees &amp; Contractors</td>
<td>Informed about laptop policies</td>
</tr>
</tbody>
</table>
Identify “Your” Gaps

Gap Analysis

• Gather data about your environment
• Analyze according to your
  – Risk management strategy
  – Risk classification
  – Risk tolerance

The highest risk for your business is not knowing where your risks are or how well prepared you are to manage the affects of adverse events
Protect: Identify Next Steps

Make informed decisions about managing identified risks!
Protect: Invest in Prevention

01  Know your data!

02  Invest in secure access

03  Conduct awareness training

04  Implement layered defense
Detect: Arm Yourself

01 Vulnerability management

02 Anti virus

03 Firewalls

04 Intrusion Protection
Respond: Have a Playbook Ready

01 Coordinate with stakeholders

02 Analyze response & recovery

03 Execute containment activities
Recover: Prepare to Recover

01 Implement recovery plan

02 Restore operations

03 Capture lessons learned

04 Update playbook
IRM_ A Continuous Process

1. identify
2. protect
3. detect
4. respond
5. recover

From the NIST Cybersecurity Framework
Next Steps
How do you eat an elephant?
One bite at a time....
Q & A
Thank You

www.talatek.com