Cybersecurity
FOR SMALL BUSINESS

Jason Pekovitch
Director of Development

MEDA Spring 2018 Conference

Montana Interactive
The 2017 State SMB Cybersecurity report indicates that 61% of small and medium businesses have experienced a cyber attack in the last 12 months.

Cyber attacks cost small and medium businesses between $84,000 and $148,000 on average.

60% of small businesses go out of business within six months of a significant attack.

90% of small business don’t use any data protection at all for company and customer information.

58% of SMBs have no password policies, 68% do not strictly enforce them.
Cybersecurity
FOR SMALL BUSINESS

Be a Hard Target

• Your business is unlikely to be specifically targeted

• Reasons our business may be targeted
  • You made the news with political or social context
  • You are an easier target than another business with equivalent data value

• More likely a cyber attack will come in the form of
  • Phishing via phone or email
  • Self-Propagating malware
  • Ransomware

You don’t need to run faster than the bear, you just need to run faster than the other guy running from the bear
<table>
<thead>
<tr>
<th>Threats</th>
<th>Mitigation Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Denial of Service (DDOS)</td>
<td>Segregate your core business data from your web presence</td>
</tr>
<tr>
<td>Site Hijacking</td>
<td>• Use cloud hosts when possible</td>
</tr>
<tr>
<td>Data Breach</td>
<td>• Use a firewall if access is needed</td>
</tr>
<tr>
<td>OWASP Top 10</td>
<td>• Vendor Management</td>
</tr>
<tr>
<td></td>
<td>• Vet your software and hosting providers</td>
</tr>
<tr>
<td></td>
<td>• Ask for their policies and certifications</td>
</tr>
<tr>
<td></td>
<td>• Verify - It is still your responsibility</td>
</tr>
<tr>
<td></td>
<td>• Use a scanning suite or 3rd party accessor</td>
</tr>
</tbody>
</table>
## Threats

- Network Breach
  - Man in the Middle attacks
- Physical Breach
- Viruses & Malware
- Out of date software
- Missing patches

## Mitigation Strategies

- Separate business your network from the public wifi (guest network)
- Employ and internet firewall
- Keep your equipment physically secured
- Apply patches as they become available
- Use anti-virus software
  - Signature Based
  - Behavior Based (0-day threats)
# Cybersecurity

## For Small Business

<table>
<thead>
<tr>
<th>Threats</th>
<th>Mitigation Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>Create a security policy</td>
</tr>
<tr>
<td>Malware</td>
<td>Train your employees how to handle</td>
</tr>
<tr>
<td>Ransomware</td>
<td>Phishing attempts</td>
</tr>
<tr>
<td>Weak Passwords</td>
<td>Suspicious emails</td>
</tr>
<tr>
<td>Accidental Disclosure</td>
<td>Sensitive data</td>
</tr>
</tbody>
</table>

- Enforce your policies
  - Automatically when possible (passwords)
  - Manually when necessary (data handling)

- Maintain a security mindset
Cybersecurity FOR SMALL BUSINESS

Jason Pekovitch
Director of Development