

“Cyber Security for the Masses”

SMB Perspective

Chris Simpson

Email: chris@brightmoonsecurity.com

SMB Considerations

- Know where (onsite, mobile devices , etc.) your critical data is and protect it
 - SSN's, Medical info, Credit cards, Intellectual property
- Limited Budget
 - Leverage free information
 - NIST, SOeC, Local security organizations
 - Consider cloud services for “economies of scale”
 - Leverage “big company” security expertise (i.e. Google, Microsoft, Intel/McAfee, HP, etc)
- Ignore the hype
 - Follow the basics (NIST SMB Must Do's, OWASP, SANS)
- Prepare for the worst
 - Devote some resources for incident response and recovery before something happens

NIST - The “absolutely necessary”

small business security activities to protect information, systems, and networks.

- 2.1 Protect information/systems/networks from damage by viruses, spyware, and other malicious code.
- 2.2 Provide security for your Internet connection.
- 2.3 Install and activate software firewalls on all your business systems.
- 2.4 Patch your operating systems and applications.
- 2.5 Make backup copies of important business data/information
- 2.6 Control physical access to your computers and network components.
- 2.7 Secure your wireless access point and networks.
- 2.8 Train your employees in basic security principles.
- 2.9 Require individual user accounts for each employee on business computers and for business applications.
- 2.10 Limit employee access to data and information, and limit authority to install software.

NIST - Small Business Information Security: The Fundamentals

Selecting SMB Security Tools

- Selecting the right security tools and finding those tools at a reasonable price is difficult for SMB's.
- SMB's should look for tools that:
 - Prevent loss of data to remove potential legal liability
 - Prevent loss of “work hours” removing malware
 - Are free with support or low cost
 - Easy to set up and monitor
- Take the time to properly set up and monitor the tools you choose
- Investigate “Security as a Service” and Managed Security Services (I.e. Security On Demand, Metaflows etc)