



Small and Medium Business Security Roadmap

Pat Slagle, PMP and Cris DeWitt, CISSP

Information security breaches causing work stoppages, information/identity theft and a variety of other expensive attacks continue to be a problem for businesses. Small to medium sized firms (10 to 500 employees) may be even more susceptible to attack than larger ones. Smaller firms tend to have smaller IT departments, fewer technology tools and lesser trained users and employees with less separation of duties. And, many in this market are also subject to the various government (Sarbanes-Oxley, HIPAA) and business (Payment Card Industry standards) regulations requiring more robust IT controls and governance.

So how do you protect your business and address compliance issues? Take the time and use your budget appropriately to develop a secure posture with IT policies and procedures appropriate for your business. And then don't make the mistake of becoming overconfident and thinking you're job is done. It's not. Factors causing change to your plans include:

- New attacks surfacing almost daily
- New assets purchased
- Changing business objectives
- Employee turnover

In-Depth Security has developed the following roadmap and project plan outlining recommended activities and the frequency with which they should be performed to help you develop and maintain this secure posture.

Secure Posture Roadmap

1. *Develop/Refine IT Policies:* The foundation of ALL secure business is clear and comprehensive IT and security policies. Review what you have and develop what you don't. Make sure they accurately reflect your business priorities and cover appropriate legal requirements as they relate to your business. Review them at least annually and communicate them often.
2. *Review Network Architecture:* Due to the changing nature of IT networks, vulnerabilities arise due to changing configurations, new devices and moving assets. Review your network architecture with a security expert annually to identify and implement new technologies and processes to correct these vulnerabilities.
3. *External Vulnerability Assessment:* Have all publicly facing (i.e. Internet facing) devices scanned and analyzed for new weaknesses quarterly. With the preponderance of new attacks being developed almost daily, it's important to keep these devices "tuned" for security. Also note that government and some business entity regulations require periodic testing.
4. *Internal Vulnerability Assessment:* Even if your perimeter network is secure, vulnerabilities may still exist on your internal network. Scan and analyze your internal network annually, possibly quarterly depending on your size, for vulnerabilities in configurations of workstations, servers, routers and other network or security appliances.
5. *Wireless Network Assessment:* Wireless networks represent an easy target for intruders. Have your wireless network analyzed quarterly for rouge devices, weak policies and other security flaws.



6. *Physical Security Assessment:* Most technology based controls can be circumvented if an attacker gains physical access to those devices. Have your business site assessed and analyzed for vulnerabilities annually.
7. *Security Awareness Training:* FBI statistics indicate that the majority of information security breaches occur from inside the business. While most of these are not malicious in intent, they are damaging none the less. Consistent communication and training on security policies and procedures will go a long way in reducing these breaches and at a reasonable cost. Quarterly, and possibly monthly, security training is recommended.

This roadmap is not intended to be the end all answer to all SMB security solutions. It does however represent best practices as recommended by In-Depth and industry experts. For a more detailed project plan with high level task associated with this roadmap, please visit www.indepthsec.com/resources_whitepapers.html.