When Selecting An IT Security Partner…

(Key Considerations For A Good Business Decision)

Losses due to electronic security breaches are devastating. Advanced Persistent Threats (APTs), along with IT Governance, Risk and Compliance (GRC) requirements, continue to grow in number and sophistication. The data suggest most organizations are not prepared to protect against, detect and respond to current security threats:[1]

- 243 = the average days a company suffers compromise before detection
- 78% = the percentage of breaches involving unique APT binaries
- 63% = the percentage of breaches detected by an external party

☑ **Look for extensive infrastructure expertise.** Security firms must be adept at not only assessing, but also designing and implementing advanced IT infrastructure. Every device on the network should support an overall architecture that strengthens your organization's security posture. Ask for examples of how the firm architects and deploys network and compute technology that could help you protect against advanced security threats.

☑ **Look for expertise around Confidentiality, Integrity and Availability (CIA).** Data confidentiality, integrity and availability represent the core of any competent security practice. Ask for examples of architecture deployments that embody all three tenets of CIA.

☑ **Look for GRC expertise.** The question today is not whether your organization has been breached, but does it know it and can it respond adequately. Technology alone cannot effectively address this issue – it must also encompass people and process and how all three relate to IT governance, risk and compliance. Look for a firm that is well versed in GRC standards because they contain best practices across the broader spectrum of people, process and technology.

☑ **Look for APT penetration capabilities.** To thwart a hacker, you need a partner who can think like one on your behalf. Does the firm have capabilities that are commensurate with the current Advanced Persistent Threat landscape? Have they successfully performed social media exploits? Do they have extensive experience conducting targeted spear phishing attacks? Have they written custom malware that evades anti-virus software? If not, ask them how they will help you defend against APTs.

☑ **Look for managed services capabilities.** At some point your organization may lack the internal knowledge, skills and/or time to maintain portions of your infrastructure or just be in need of competent external help. Look for firms that manage the solutions they sell.

☑ **Look for competitive advantages.** The former CEO of General Electric, Jack Welch, once said, "If you don't have a competitive advantage, don't compete." Ask the firm to give you their top 3 competitive advantages and evaluate those advantages in terms of their importance to you.

☑ **Look for how your data will be protected.** The company you partner with will have access to confidential information concerning your IT environment that, if compromised, could cripple your organization. Have them explain where they store your information and how they protect it. Ask to see their internal security policies and procedures.

☑ **Look for financial stability.** Does the company you are considering working with have the financial staying power to weather inevitable downturns in the economy? Ask the firm for their debt-to-equity ratio and cash headroom (how many months they could survive without making a sale). Any firm who will not readily share this information may be trying to hide something.

☑ **Look for core values alignment.** A true partner functions as an extension of your IT staff and should have values and beliefs that align with those of your own organization. Ask for documentation that will give you insight into the firm's corporate culture and help you learn about their key commitments.

[1] *Mandiant 2013 Threat Report*