POSTER: Practitioners Session

Small Businesses are Between a Cyber-Rock and a Cyber-Hard-Place

John R. Budenske
Cyberific Secure Autonomous Systems Ltd.
Edina Minnesota, USA
John.R.Budenske@IEEE.org

***Abstract*— This poster presentation will provide a cyber-security practitioner's experiences and insights into the challenges that small businesses face in attempting to deal with cyber threats and attacks. Though definitions differ, in general, a Small-to-Midsize Business (SMB) is viewed as having less than 1,000 employees. A “small” business is often viewed as having fewer than 100 employees. Very small or Small-Office/Home-Office (SOHO) or “micro” businesses (as they are starting to be called) are viewed as having less than 10 employees. Each of these sizes of SMB has their own different IT requirements, and often faces different IT challenges as compared to larger enterprises. The smaller the business, usually the more tightly constrained are its resources (budget, staff, training). Needless to say, this IT constraint projects directly onto the SMB’s cyber-security needs. Our focus here is on the small to micro size business.**

By most accounts, the cyber-security deck is stacked against midsize, small, and micro businesses. Collectively, the gathered statistics show that cyber criminals are increasing their attacks upon smaller businesses due to they're being easier targets.

Ransomware alone hit one third of SMB worldwide in 2016. In general, one fifth of companies that are hit by any malware have to completely stop operation immediately; a cost that can set a company back significantly. In fact, the average time for a small business to recover to normal operation is over a week, and the average cost for a small business to clean up after the hacking is estimated to be over $700,000. If you consider that nearly half of all cyber-attacks worldwide are against businesses with less than 250 employees, it’s no wonder that a significant percentage of them end up closing down within six months after a cyber-attack (some sources claim shut-downs to be as high as 60%).

Small businesses know that they are between a cyber-rock and a cyber-hard-place. But they often cite that they have little time and even less resources to address the issue. Cyber-security tools, and training their employees on them is costly. Many micro businesses do not even have a trained IT person on the payroll; some might have a rent-an-IT-contractor on call, or have one stop by every few weeks to keep their computers running. Small and micro businesses need cyber help.

Currently, there are four different bills in the U.S. Congress to have the Small Business Administration (SBA) and/or the National Institute of Standards and Technology (NIST) provide additional Cyber-security support, tools, and training to small businesses. It’s unclear if any of them will become law. The question for cyber-security experts, researchers, and policy-makers is how to apply aid and resources (technology, funding, training) such to make it easier for the smaller businesses to embrace their adoption of cyber security?

There is not abundant published insight into what it takes to convince a small or micro business to invest in an adequate level of cyber protection. In our experiences, risk analysis and management approaches (often used in applying cyber security principles) can help a small business owner better understand what risks they are facing. Unfortunately, it may only serve to give them more sleepless, worrisome nights than to propel them to allocate money, time, and resources that they did not have in the first place.

Cyber-security tool vendors view the micro-size business market as not a very vibrant one, especially for sophisticated tools that are costly and require an investment in training. Cyber-security service providers face two challenges. First, the service needs to continually show benefit otherwise the business owner might lower the priority to pay for the service when money is tight; and second, many cyber-security service providers only focus on one aspect of security (like email filtering, secure cloud service, or more active anti-virus protection), and does not provide comprehensive security. The business owner is easily confused or befuddled by needing multiple (possibly expensive) cyber-security services. The small business owner's lack of understanding cyber-security can itself be an obstacle.

Small and micro businesses are challenged with a lack of knowledge, funding, time, and resources. This presentation will further describe the criteria that many small and micro businesses require in order to consider adopting a cyber security policy and investing in tools and training.

Keywords— security practitioner, SMB, small business, micro business, cyber-security, SBA, NIST, malware, ransomware, hacking.