Who's Protecting America's Small Business?

Too often, the "engine" of the U.S. economy remains vulnerable

By Bob Hayes

You hear it all the time from our political and economic leaders — small business is the engine of the U.S. economy. Of the nation's 26.8 million businesses, some 99.9 percent of them have fewer than 500 employees, according to the U.S. Census Bureau.

In addition to driving the economy, small business is the source of a big share of the nation's innovation. For example, 98 percent of telecommunications patents and 97 percent of software patents are issued to companies of 500 or fewer companies, according to a U.S. Small Business Administration study.

Unfortunately, these small businesses tend to pay little attention to security issues — often because they lack the resources. The innovation typical of small businesses could be a target of foreigners or others seeking to steal trade secrets, yet these companies are among the least likely to take measures to protect themselves. The lack of security among small businesses even puts big businesses at risk, especially large companies that interact with hundreds of smaller companies as critical elements in their supply chains.

There are several reasons why small businesses remain soft targets in a time when security efforts at larger companies are greater than ever. The sheer number of small businesses suggests a need for security solutions that are scalable and easily replicated, however, such solutions are mostly lacking. Some approaches to the problem have shown promise, but the nation's small businesses still remain largely vulnerable because few solutions have proven scalable.

Why Small Business Is At Risk

It is easy to point to reasons why small businesses lack sufficient security. Here are a few:

- **Lack of resources.** Small businesses are often small because they are still looking for the keys to success; that is, to becoming large businesses. By definition, a small business has fewer resources, and discretionary expenditures often come out of the owner's pocket.
- **Lack of security awareness.** Small businesses are often content to ignore issues of security or business continuity. Even standards and regulations are less likely to be enforced among small businesses. The result is that security becomes an optional expense.
- **No security "champion."** In small business, everyone wears many hats, and the security hat may be one that is never assigned. If the CEO is also the chief marketing officer or in charge of Human Resources, he is unlikely to have the time or inclination to take on additional duties. The result is that there is no champion of the security cause — and security evolves in a reactive, rather than proactive, manner.
- **Suppliers target larger customers.** One industry supplier concedes that 99 percent of its business comes from Fortune 500 companies. From a completely capitalistic perspective, it makes sense that a supplier would pursue the business that is the most lucrative and profitable. Dealing with a handful of top companies involves less work than pursuing millions of onesy-twosy applications.
- **A higher threshold of security sensitivity.** A small business's security sensitivity does not typically extend to threats or vulnerabilities, but instead tends to center on specific events, usually after they have occurred.

Who Should Be Helping Small Business?

The Federal Government has targeted some resources to small businesses, such as the Ready.gov and FEMA Web sites, but it is questionable to what extent businesses are aware of and taking advantage of the resources.

Security-focused committees of industry organizations — such as those serving the food or chemical industries — and even organizations that purport to serve small business, such as the Chamber of Commerce and the National Federation of Independent Business, tend to have more involvement by representatives of larger companies, thus tending to skew their missions toward big-company concerns.

As technology suppliers target primarily larger end-user companies, even the industry magazines and Web sites tend to focus circulation efforts to recruit larger end-users as a way of appealing to advertisers. They also seek to target their circulation to specific, security-related job titles, a practice that unintentionally favors larger companies where security roles are more clearly defined.

The same big-company strategy also extends to trade show attendance, which is promoted more strongly among big potential customers. Even professional security organizations are targeted more to "full-time" security professionals rather than those for whom security is one of many functions. In general, security education and information about technology are less likely to be available as valuable security tools to small businesses.

Some large companies have embraced a role to promote security among small business, especially companies that are part of their supply chain. Large suppliers might require a supply chain certification that would point to specific vulnerabilities and guide small businesses to address them. However, there are obstacles to additional involvement of large companies in the security of small businesses, including possible civil liability, regulatory requirements and costs.

Businesses that import products also often seek Customs-Trade Partnership Against Terrorism (C-TPAT) certification, a program that seeks strategically to secure and facilitate international trade. Such certification minimizes the need for products to sit waiting for a customs inspection; therefore, they arrive sooner. C-TPAT certification and supply chain certifications can help to guide small businesses toward a more strategic view of security.

Some Approaches with Promise

Public-private partnerships have also emerged as a tool to boost the security of small businesses. Here are some examples:

Michigan State University (MSU) Critical Incident Protocol (CIPS) Community Facilitation Program.

The sheer number of small businesses suggests a need for security solutions that are scalable and easily replicated; however, such solutions are mostly lacking.

Under a federal grant, MSU created its CIP program to "enhance cities', counties' and regions' capabilities to prepare for, respond to and recover from man-made and natural disasters through public and private sector collaboration, communication and cooperation."

The public-private partnership for joint management of critical incidents provides a channel for participation by small businesses in programs initiated in 47 communities in 24 states with 4,200 participants. When federal funding for the program ended last year, CIP began an initiative partnering with the Security Executive Council. Involvement by the MSU School of Criminal Justice provides expertise on a variety of subjects that could enhance business continuity, government continuity of operations, security, risk management, crisis management and emergency preparedness. MSU faculty members offer expertise in brand protection, hiring/recruitment/retention, security, domestic terrorism, risk/threat assessment, critical incident planning, identity theft and others.

Target/Safe City Program. Large retailer Target leads a community-based initiative to leverage partnerships and technology to help communities and businesses reduce crime and create an environment where people feel safe and secure. The collaborative effort involves area retailers, community organizations and business and property management. By combining resources through programs like these, small businesses are able to access technologies and information-sharing opportunities they otherwise could not. And the community focus on safety and security benefits all community stakeholders. Target's approach is to share resources and expertise to build safer, more vibrant communities.

COPS Bureau / Los Angeles. Community-oriented policing services (COPS) bureaus provide a means for police departments to focus on crime trends impacting neighborhoods. At the COPS Bureau in Los Angeles, for example, the focus is on specific enforcement against criminal actions identified by community stakeholders. The bureau uses any and all Los Angeles County resources to impact the crime in a specific neighborhood or area. This narrow geographic focus gives neighborhood small businesses the ear of local law enforcement, developing relationships and making their security concerns known.

By using a "face-to-face" approach, the LA COPS Bureau deputies remove a barrier that formed over time between law enforcement and the neighborhoods they patrol. COPS deputies work alongside community stakeholders to gain their trust and learn about a variety of issues concerning the neighborhood and its businesses.

Business Improvement Districts. Self-imposed tax zones, in which businesses pay a fee to help fund community improvements, offer another opportunity for small businesses to leverage pooled resources for improved safety and security. Downtown Improvement Districts in cities like Atlanta and Philadelphia have enacted measurable security results by doing such things as deploying uniformed

"The benefits of security investment play up and down the supply chain from the farmer to the cooperative, roaster, distributor and retailer. World-class beverage quality is both the end and means to enable protection." **— Francis D'Addario**

ambassadors, launching targeted security strategies, holding events and beautifying the area to deter crime. All of this assists local small business.

Corporate Responsibility

Francis D'Addario, formerly vice president of partner and asset protection at Starbucks Coffee Company, sees a corporate responsibility for large companies that includes ethical conduct tied inextricably to strategic performance. That "care culture" can help to mitigate risk for people, products and processes up and down the supply chain, including small businesses. Results of such an approach include higher stakeholder engagement, consumer confidence, as well as quality and earnings assurance.

Now a member of the faculty of the Security Executive Council, D'Addario recalls applying the principles of corporate responsibility throughout the supply chain during his tenure at Starbucks. "The health and safety of coffee and tea buyers are strategically essential to Starbucks," he said. "These clients arguably represented the finest palates, agronomy and logistics talent in the world." Starbucks was looking at growth from 4 to 44 percent in the use of the world's highest quality Arabica coffee in five years, and focused on security of the supply chain as a corporate priority.

"Buyers are emissaries to the farmers for Coffee and Farmer Equity (C.A.F.E.) practices," D'Addario explains in his book, *Not a Moment to Lose…Influencing Global Security One Community at a Time*. "They provide resources to incrementally improve the agronomy, crop quality and community with transparent premium pricing tied to performance objectives. Consumer confidence for 5 million customer transactions per week depends on the safe transport of buyers and products around the globe. The benefits of security investment play up and down the supply chain from the farmer to the cooperative, roaster, distributor and retailer. World-class beverage quality is both the end and means to enable protection. It affords livelihoods for several hundred thousand stakeholders."

Better Approaches Needed

A problem with small business security approaches to date is a lack of scalability. Ideas abound throughout the various government programs and public-private partnerships, but unfortunately a vast percentage of small businesses have been touched by neither. Lacking are both a means of raising awareness among small business of the strategic importance of security and a means of making widespread resources available to boost the security of this critical strategic component of the U.S. economy.

There is a real risk that the nation's gap in small business security, like many security problems, will not be addressed until it is too late. In today's media-driven culture, a single random attack on a small business could cause widespread panic that could undermine the nation's economy.

The Security Executive Council is conducting research to identify security solutions and strategies for small business. We are encouraging input and looking for stories of small business security success. Please share your ideas by emailing contact@secleader.com. ▮

Bob Hayes is Managing Director of the Security Executive Council. He has more than 25 years of experience in security, including eight years as the CSO at Georgia Pacific and nine years as security operations manager at 3M. The Council works with Tier 1 Security Leaders™ to reduce risk and add to corporate profitability in the process. It serves all aspects of the security community through its pioneering Collective Knowledge™ approach. A faculty of more than 100 experienced security executives provides strategy, insight and proven practices that cannot be found anywhere else. To learn about becoming involved, e-mail contact@secleader.com or visit www.securityexecutivecouncil.com/?sourceCode=std.

Security in a Box

Among the resources offered by the Security Executive Council for small businesses is a collection of time-tested and proven guidance for building or enhancing a security risk mitigation program. "Adding Business Value by Managing Security Risks" is a binder and accompanying CD that provides a baseline for security practice for any organization. It is "security in a box" and the CD contains actual program elements, documentation, examples, templates, outlines, presentations and other components that correspond to the topics covered in the book and which can be adapted for use within any security program. For information, visit https://www.securityexecutivecouncil.com/abv.