# Data Security is Mission-critical for all Businesses Regardless of Size

By Kelly Gates, Gates and Company

Poor website and web application coding can allow hackers unauthorized and destructive access to databases and networks.  According to FBI Director James Comey, "There are two kinds of big companies in the United States. There are those who've been hacked…and those who don't know they've been hacked."

Small- and medium-sized businesses typically cannot afford a full-time IT department nor the typically high fees charged by 24/7 Internet and WAF security firms that big companies have the luxury to afford. These financial restrictions are forcing small and medium-sized companies to seek smarter and more cost effective alternatives for high quality website security.

SQL [Structured Query Language] injection is currently the most common form of website attack.  This kind of exploitation is easy enough to accomplish by an inexperienced hacker. SQL injection in the hands of a highly skilled hacker can exploit website coding weaknesses allowing them access to web servers.

Although not all successful hack attacks use SQL injection, many do.   The vulnerability to SQL injection is well understood.  A study conducted by the Poneman Institute found that SQL injection remains a pervasive threat where 65% of respondents stated that they experienced one or more SQL injection attacks that invaded their perimeter defense in the past 12 months.  This same study also determined that there is a lack of real-time detection for SQL injection attacks, where it takes approximately 140 days for an organization to detect an attack, on average.  The study also noted that 40% of respondents stated that it took six months or longer to detect an attack and an additional 68 days, on average, to actually remediate the attack.

**Small- and Medium-sized Businesses are Targets, Too**

Data security and website breaches occur daily all around the world.   A story in *USA Today* headlined "Hacking a big danger for small businesses" says big companies are not the only ones that get hacked. story states, "the costs associated with computer and website attacks can run well into the thousands and even millions of dollars for a small company.  According to a 2013 survey by the National Small Business Association, 44% of small businesses have been attacked at one time or another.  Those companies had costs averaging $8,700."

A recent article in the January 21, 2015, U.S. edition of *The Guardian* states that "cybercrime and hacking are even bigger worries for small business owners.  Hacks cost the American economy $1 billion per year and it's not just the Sony Pictures and Targets of the world."  The article also states, "a report from McAfee found almost 90% of small- and medium-sized businesses in the U.S. do not use data protection for company and customer information, and less than half secured company email to prevent phishing scams."  The article continues, "according to a PwC report, the average cost of a firm's worst security breach is rising significantly.  For some small- and medium-sized businesses, the worst breaches cost between ~$100,000 and ~$180,000, on average", providing yet another data point on how expensive data security and website breaches can become.

## Hackers are More and More Sophisticated

The last year has seen an increasing number of sophisticated and ever-larger hacks on corporate and Federal government networks and social media accounts. In October 2014, Staples reported that hackers broke into the company's network and compromised the information of about 1.16 million credit cards. In the summer of 2014, JPMorgan Chase said hackers had compromised some of the personal information of 83 million households and small businesses. More recently, in February 2015, Anthem Blue Cross said its database had been hacked, potentially exposing personal information of about 80 million of its customers and employees.

Other recent hacks were also suffered by reputable companies, including Ebay, Living Social, Adobe, Home Depot, AOL, Scribd, Target, Apple, Sally Beauty, Neiman Marcus, UPS, Michael's, Snapchat, and Nintendo. If these large, well-known, brand-name companies can be hacked, what does this mean for small- and medium-sized businesses that cannot afford dedicated IT departments?

## Mitigate Your Risk and Cost of a Hack Attack

Small and medium-sized businesses can be particularly vulnerable because they do not have budgets for a full-time, dedicated IT staff or expensive security software programs or 24/7 human-based monitoring. Yet, safeguarding your business against security breaches and threats does not necessarily require hiring a full-time IT staff. In fact, protection from hackers can be very affordable and extremely reliable.

---

One solution is **dotAlert,** which gives IT administrators the ability to instantly block attacks on their systems via their mobile device simply by blocking the IP address of the attacker.

Working in conjunction with dotDefender, **dotAlert** provides an easy to use central management console to customize and prioritize alerts based on factors such as type of attack, severity, velocity, source and time of day of attack. For more information on **dotAlert,** *visit www.dotalert.com for a free 30-day trial.*

---

Kelly Gates is Managing Director with Gates and Company, an international management consulting and investment banking firm dedicated to helping companies profitably expand their business and realize gains on growth initiatives. Ms. Gates helps firms with market and competitive analysis, business plan development, strategic marketing and positioning, strategic planning, channel strategy, new product introduction, market entry, and M&A activities. kgates@gatesandcompany.com