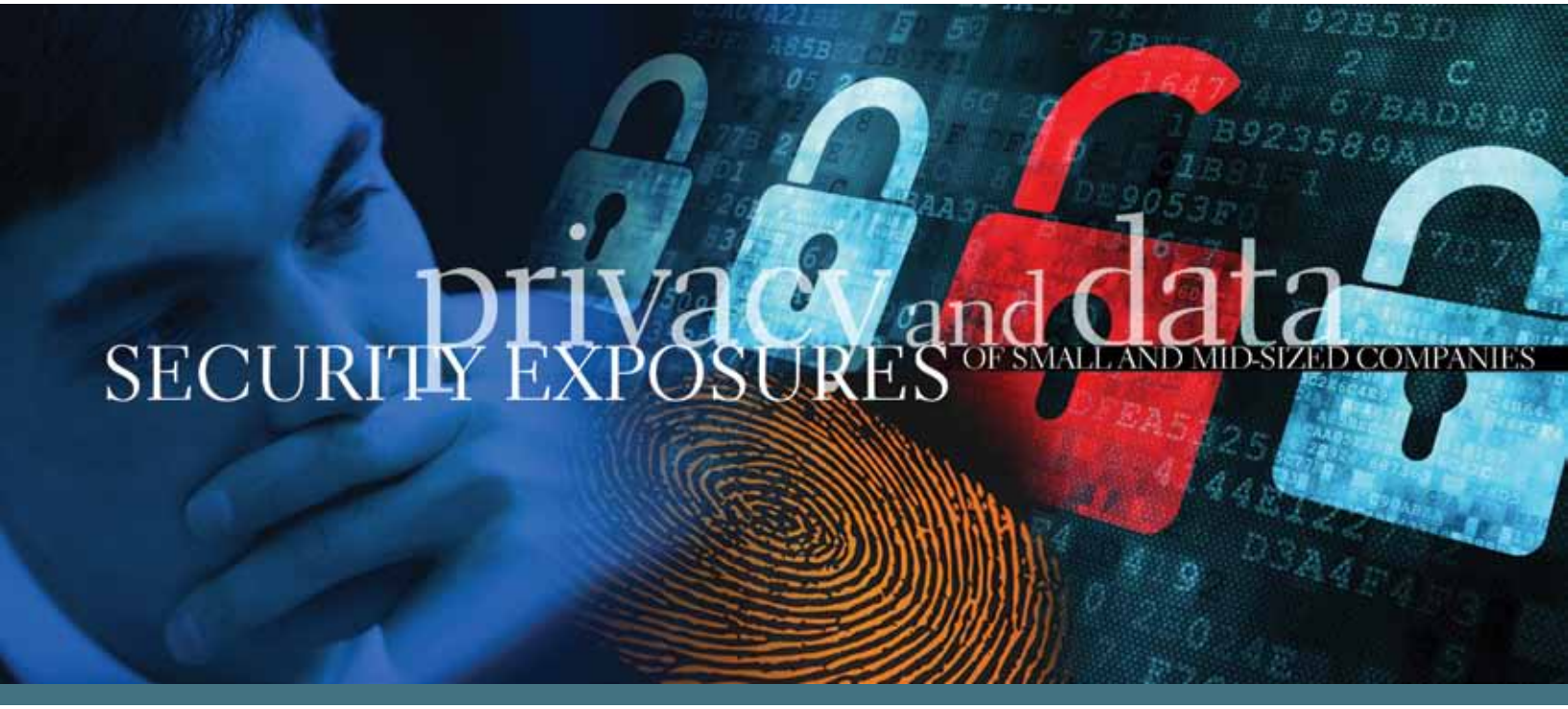
ADVISEN
Insurance Intelligence



PRIVACY AND DATA SECURITY EXPOSURES
OF SMALL AND MID-SIZED COMPANIES

December 2012

Sponsored by:

XL

PRIVACY AND DATA SECURITY EXPOSURES
OF SMALL AND MID-SIZED COMPANIES

Almost every company will eventually have important data lost or stolen, whether the result of an attack by a hacker, a lost memory stick or smartphone, or a stolen laptop. How well prepared a company is to deal with such a situation could mean the difference between a bump along the business highway or a bankruptcy-threatening calamity.

Owners and managers of small and midsize businesses (SMBs) often dismiss the threat of data breaches.[1] That is unfortunate since they are increasingly vulnerable to having data lost or stolen. SMBs, in fact, have become a favorite target of hackers.

During the first six months of 2012, more than a third of targeted attacks on businesses were directed toward companies with fewer than 250 employees, according to security vendor Symantec.

Organized crime views smaller companies as high-reward and low-risk targets. According to Verizon's *2012 Data Breach Investigations Report*, the focus on small companies is an outcome of "industrialized" attacks that can be carried out against large numbers of targets with little resistance from the victims. Smaller businesses are typically less sophisticated in their defenses and therefore are ideal targets for such raids. "Thus, the number of victims in this category continues to swell," according to the report.[2]

During the first six months of 2012, more than a third of targeted attacks on businesses were directed toward companies with fewer than 250 employees, according to security vendor Symantec. That was double the percentage of attacks aimed at similar sized companies at the end of 2011.[3] Visa reports an even more alarming statistic: 85 percent of all data breaches occur at the small business level.[4] Trustwave, an internet security firm, claims that 92 percent of credit card data compromises take place in small businesses with low processing volume.[5]

One study found that a laptop is stolen every 53 seconds, and that 70 million smartphones are lost each year.

Hackers grab the headlines, but they are only one cause of compromised information. Lost or stolen laptops, smartphones and memory sticks account for a significant portion of compromised records. One study found that a laptop is stolen every 53 seconds, and that 70 million smartphones are lost each year.[6] Many people use their personal devices for work as well, so even an iPad used largely for recreational purposes could be carrying sensitive business emails, contact information, proprietary reports, passwords to protected work websites, and other critical information – often with only the most rudimental security measures.

The costs of a data breach

A data breach can be devastating for any company, but it can be especially so for a small company. While costs vary by the type of data involved and other factors, an often-cited figure from the Ponemon Institute is an average of $194 per record. Organizations having their first data breach spend on average $37 more per record than companies that had previously experienced a breach.[7]

Costs arising from a data breach can include forensic IT expenses, fines, credit monitoring and identity restoration, crisis management activities and attorney fees. One significant cost is notifying affected people of the breach. Presently 46 states have data breach notification laws. The average cost to notify victims of a breach is well over $500,000, according to the 2011 Cost of a Data Breach Study: United States.[8]

A significant risk for small and midsize organizations is losing business as a result of a breach. A survey by Javelin Strategy & Research found that more than half of breach victims reported diminished confidence in an organization's ability to protect and manage their personal data following a breach, and 30 percent elected to never purchase goods or services again from that organization.[9]

An alarming new risk for companies of all sizes is the threat of damages being awarded to victims who collectively bring suit against organizations experiencing a breach, even though the victims do not yet have demonstrable losses. Courts typically dismiss lawsuits stemming from data breaches unless victims can prove specific damages, but in a few significant cases judges have denied motions to dismiss in lawsuits that demonstrate a possibility of future damages.[10] In *Anderson v. Hannaford*, for example, a case which concerned compromised

The Better Business Bureau (BBB), in partnership with Visa, Symantec and Kroll, has developed practical data security guidelines for SMBs, which can be found on the BBB's website.

credit card data, the Federal District Court in Maine determined that damages resulting from the breach were not recoverable under Maine law because losses were speculative and not reasonably foreseeable as consequences of the defendant's alleged negligence and breach of contract. On appeal, however, the First Circuit Court reversed the district court decision and held that card-replacement and credit-insurance costs were sufficient to state a claim and for the case to proceed to discovery and summary judgment. Defense lawyers have expressed concern that the plaintiffs' bar will likely attempt to broaden this holding to apply at least to other mitigation costs incurred by plaintiffs, with more litigation advancing beyond the motion-to-dismiss stage.[11] Scott Schleicher, XL Group's technology and cyber risk underwriting manager, describes this emerging risk as being significant enough to potentially cause market capacity to shrink and rates to increase.

Cybercrime is not limited to stolen data. Cyber-extortion also is on the rise. In one extortion scheme, a criminal breaks into a system and encrypts the company's data. The data is essentially held hostage until a ransom is paid.

On the defense

So many SMBs fall victim to cybercriminals because many are simply easy prey. Symantec reports that 33 percent of small businesses lack even basic antivirus protection.[12] Fortunately companies can take steps to avoid data breaches, and to lessen the consequences once one occurs.

The Better Business Bureau (BBB), in partnership with Visa, Symantec and Kroll, has developed practical data security guidelines for SMBs, which can be found on the BBB's website.[13] According to the BBB, not only should SMBs develop a data protection plan, they should openly communicate it and actively implement it as a way to build customer trust. Despite best efforts to protect data, information will be lost or stolen. SMBs need to be prepared for that very likely event and know what to do if they believe they've been a victim of a data compromise. Without advance preparation, a serious breach can quickly mushroom out of control with potentially disastrous consequences. Some important features of a disaster response plan include being prepared to immediately take action to prevent further damage, knowing who to contact (lawyers, law enforcement officials, affected companies such as banks, regulatory agencies, etc.), and understanding the type and quantity of information stored and the associated notification requirements.

At an average cost of $194 per compromised record, even a comparatively small business could conceivably run up a tab in the hundreds of thousands, or even millions of dollars, as a consequence of a data breach

Insurance

At an average cost of $194 per compromised record, even a comparatively small business could conceivably run up a tab in the hundreds of thousands, or even millions of dollars, as a consequence of a data breach. SMBs can take steps to lower the likelihood of a breach and contain costs following one, but it is increasingly clear to many companies and their brokers or agents that insurance is not only a wise purchase, it is a necessary one.

What is frequently called cyber liability insurance is in fact a package of coverages protecting companies against both first-party and third-party losses arising from a data breach or other event as defined in the policy. While policies have become somewhat more standardized over the years, coverage still varies considerably by carrier.

Common first-party coverages include:

- Loss of digital assets;
- Business interruption and extra expense;
- Expenses arising from cyber extortion; and
- Security event costs such as notification expenses and credit monitoring costs, as well as costs of various consultants such as a forensic IT expert and a public relations firm.

Frequently found third-party coverages include:

- Network security and privacy liability; and
- Electronic media liability, including liable, defamation; and copyright and trademark infringement.

Conclusion

The probability of a data breach – potentially with dire consequences – increases daily for SMBs. Most SMB owners and managers, however, continue to believe that data security is a large company problem, and many do not take even rudimentary steps to keep their data safe. However, even basic data security measures could deter a breach since cybercriminals know that there are so many other unprotected targets available to them.

Although most SMBs can do much more to protect their data, even the most diligent company can have a breach incident. Being prepared to respond to a breach can mean the difference between quickly gaining control of the situation with minimal financial and reputational damage, and helplessly watch events spiral out of control. Insurance is an important tool to assure that SMBs not only have protection against financial loss, but that they also have the resources to take charge of a breach situation and minimize its impact. ■

NOTES:

1 "Data Breach - What are the Risks to My Company?" Jaburg Wilk http://www.jdsupra.com/legalnews/data-breach-what-are-the-risks-to-my-c-58826/

2 2012 Data Breach Investigations Report, Verizon http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

3 Hackers increasingly zero in on small businesses, Symantec says http://www.csoonline.com/article/712942/hackers-increasingly-zero-in-on-small-businesses-symantec-says

4 "Intro to Small Businesses: It's About Trust," Better Business Bureau http://www.bbb.org/data-security/intro-to-small-businesses/

5 "How Compliance Affects You," Compliance Facts http://www.compliancefacts.com/public/index

6 "Cost of Stolen or Lost Laptops, Tablets & Smartphones", Kensington, (2011), http://blog.kensington.com/wp-content/ktg/docs/m1_iphone_theft_banner.pdf

7 2011 Cost of a Data Breach Study: United States, Ponemon Institute http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US

8 2011 Cost of a Data Breach Study: United States, Ponemon Institute http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US

9 Consumer Survey on Data Breach Notification http://www.docstoc.com/docs/952213/2620_Javelin-Research-Consumer-Survey-Data-Breach-Notification-June-2008

10 "Courts widening view of data breach damages, lawyers say," CSO Magazine http://www.csoonline.com/article/720128/courts-widening-view-of-data-breach-damages-lawyers-say

11 Donna L. Wilson and John W. McGuinness, "Case Study: Anderson v. Hannaford Brothers," Buckley Sandler LLP http://buckleysandler.com/news-detail/case-study-anderson-v-hannaford-brothers

12 Small and Midsize Business Protection Guide: close the protection gap and safeguard your business future, Symantec http://eval.symantec.com/mktginfo/enterprise/other_resources/b-smb_pg_close_protgap_20050014_hires.en-us.pdf

13 "Intro to Small Businesses: It's About Trust," Better Business Bureau http://www.bbb.org/data-security/intro-to-small-businesses/