

Small financial, health-care service providers are targets for cybercrime

Millions of very small businesses with fewer than 20 employees, ranging from dentist's offices, financial advisors, independent legal counsellors, IT consulting firms, and other companies are focused on their core competency and win by that. At the same time many of them can neglect the security of their IT equipment and put their customers, and the future of their businesses, at risk.



Image: [Free Digital Photos](#)

Verizon's 2013 Data Breach Investigations Report, which includes data from worldwide forensic investigations, found that the 621 data breaches analysed, 193 breaches - more than 30% - occurred at companies with 100 or fewer employees.

A survey conducted by PricewaterhouseCoopers in 2013 for the UK's Department for Business Innovation & Skills, found a 76% increase with the number of breaches in small and medium-sized firms. Of those small businesses that were attacked the last year, 15% confirmed unauthorised access to business data was gained, and 9% admitted that intellectual property was stolen. While the amount of money earned from a successful breach of a small business might not be as large as a massive breach of a major corporation, the ease of hacking smaller companies means cybercriminals can simply increase the number of their attacks to collect massive profits.

The results of security oversights for very small businesses can be devastating, and small businesses that provide financial services and health-care services are among the most highly targeted by cybercriminals. In both sectors, customers trust these businesses with a great deal of sensitive information - medical records, payment and bank details, or other confidential information. For financial and health-care service providers, the consequences of such attacks are plentiful, including damage to their business reputations and the loss of angry or worried customers, along with computer network downtime that cripples their ability to function. Small businesses in these sectors also must worry about potential legal action and costly fines if the result of the data breach violated any government and industry regulations.

Hindered by limited budgets

Cybercrime has become the second most frequent type of economic crime being experienced by financial services companies, after asset misappropriation, according to PricewaterhouseCoopers. Although financial institutions benefit from regulatory requirements and industry regulations designed to safeguard customer data, very small financial service providers are hindered by limited budgets and lack of expertise when protecting their customer information. Combined with the online connectivity and convenience that most customers demand, these businesses face a real challenge. These businesses are obvious targets for cybercriminals who seek to steal stored credit card information, credentials, and bank account details from customers.

For any growing company, successfully earning the account of a well-known business is a milestone in its growth. For small financial service providers, managing the taxes of a local grocery store or helping process the payroll for local charities is a sign of growth, and many will list their clients on their websites. But for cybercriminals, this can be an opportunity to attack the smaller business as a way to gain access to the larger clients.

A clear interest in targeting health care

As if financial records aren't sensitive enough, there are few things more sensitive than the health-care records often stored by small dentist offices, physical therapists, and other independent health-care providers. An IT security breach in these organisations will not just compromise patient data, but will also undoubtedly damage the trust of any patients.

Cybercriminals have a clear interest in targeting health-care organisations. A 2012 study released by the Ponemon Institute revealed that 94% of hospitals in the United States had experienced at least one data breach in the previous two years. But cybercriminals aren't typically interested in reports on patient blood pressure or medication - they are after money. The report found that the information stolen largely consisted of patient billing and insurance records. Identity theft, again for the purposes of stealing money, was a common outcome.

While small health-care service providers may not have to deal with the volume of patient information found in larger hospitals, the changing nature of patient health records means they aren't immune to the threat. Health-care records have become increasingly electronic, and these records can easily make their way onto laptops and mobile devices such as smartphones and tablets. This means that, in addition to a flood of sophisticated malware targeting their computers, very small businesses must also take great care to ensure any portable computers and mobile devices containing patient medical records don't fall victim to physical theft.

Many new layers of risk

Small businesses of all types, particularly health-care and financial service providers, must have awareness of the different types of data that include customers' personally identifiable information (i.e. name, addresses, cellphone numbers, etc.); personal health information; customer information (such as credit card numbers and verification codes, billing and shipping addresses, purchasing history, shopping behaviour, etc.).

For small health-care and financial service providers Kaspersky Lab recommends using a limited number of mobile devices for business purposes. While smartphones and tablets may add some convenience and accessibility, they add many new layers of risk. If any mobile devices are used for business purposes, they must be equipped with anti-theft security features that enable remote locking and wiping of misplaced devices.

Also, data encryption is a vital component of maintaining the security of sensitive data. Encryption is not only a key technology for any mobile device, but it should also be used on desktop and laptop PCs, as well as any file servers. Very small businesses can find straightforward encryption technology in security solutions like Kaspersky Small Office Security that makes it easy to render sensitive data inaccessible to cybercriminals. Also, properly encrypted data will ensure protection from accidental deletion and unauthorised employee access as well. In fact, most financial and health-care service providers will find that data encryption is required by law.

As with any business, the foundation of IT security begins with up-to-the-minute anti-malware protection and proactive detection tools that can be found in Kaspersky Small Office Security. Another easy way to bolster security is to instil strong password discipline amongst employees. An effective way to enforce good password habits is to use a password manager that stores all employee passwords in encrypted vaults, so employees just have to remember a single "master password".

Small businesses of all types continue to be prime target for cybercriminals, and the more valuable data these businesses hold, the bigger the target they become. A single oversight by the business owner or a bad decision by an employee can allow a breach that can drive most small businesses into ruin, and with so much valuable data to steal, it stands to reason that cybercriminals, like all predators, will continue to attack targets they believe are the weakest to withstand them.