Awareness of Cyber-Security for Small Businesses

McCann Investigations
1018 Preston St.
Houston
TX 77002

Table of Content

The threath of Cyber-Attacks for Small Businesses

Small and medium-size businesses, totalling more than 28.2 million organisations, make up for 99.7 percent of all U.S. employers and create over 60 percent of all new U.S. private sector jobs. They also produce over 47 percent of the country's Gross National Product[1]. When looking at the SMB sector as a whole, it's easier to understand the importance of a healthy and secure environment business environment.

The world of cybersecurity is changing along with the world of cybercrime. The common perception among small business owners is that they are less prone to cybercrime than large enterprises. However, recent studies show how the **security threat to SMB is growing at an alarming pace**. While most SMB do hold sensitive personal data like banking information or social security numbers, they are mostly **unprepared** to keep this information safe. This makes them attractive targets when comparing the effort to the benefits of a security breach.

Smaller companies are attractive because they frequently **lack the resources and technical expertise** to maintain strong security. What could be used to target and breach an enterprise some time ago may still work on a small business now. They are also doing more business than ever online, leaving open windows for unauthorised access, and worse, possibly deploying the breach to business partners.

A 2013 study Sysmantec showed that **61% of all cyberattacks now target SMBs[2]**. Facts and figures from the report:

- Targeted attacks aimed at Small Businesses (1-250) accounted for **30 percent of targeted spear-phishing** attacks. **1 in 5 small business organisations** was targeted with at least one spear-phishing email in 2013.
- Targeted attacks aimed at Medium Businesses (251 – 2500) was similar, at 31 percent
- Only 39 percent of targeted attacks aimed at large enterprises, as compared to 50 percent in the previous year (2012). The remaining 11 percent shifted to smaller businesses
- Top industries attacked by spear-phishing: Government (16%), Services - Professional (15%), Services – Non-Traditional (14%)

1 Source: http://csrc.nist.gov/publications/nistbul/itlbul2014_05.pdf

2 Source: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

- Targeted attacks aimed at **small businesses** (1-250 employees) **in 2013 accounted for 30 percent of all such attacks**, compared with 31 percent in 2012 and 18 percent in 2011. Despite the overall average being almost unchanged, the trend shows that the **proportion of attacks at organisations of this size was increasing** throughout the year, peaking at 53 percent in November.

More recent studies (Oct. 2014) have confirmed this trend, up to labelling cyber exposure of SMBs as "**a digital pandemic**"[3]. The services sector (e.g. **healthcare, education, hospitality** etc.) has also been found to be the most targeted one.

Awareness of the Need for Cyber-Security in SMBs

These significant changes in the last couple of years have determined an obvious shift in the common perception of small business executives.

At the end of 2012, U.S. small business owners or operators still had a false sense of cybersecurity as more than three-fourths (77%) said their company was safe from cyber threats such as hackers, viruses, malware or a cybersecurity breach. At the same time, 83% had no formal cybersecurity plan[4].

The same study revealed another significant perception gap, as 83% strongly or somewhat agree that they are doing enough or making enough investments to protect customer data. At the same time, Visa Inc. reports **small businesses represent more than 90% of the payment data breaches** reported to the company.

However, two years later (2014), another survey shows a completely different perspective[5]:

- **41 percent** of our respondents were either **"extremely" or "very concerned"** that they might become a victim of cybercrime.
- A further 26 percent said that they were "moderately concerned."
- The rest of 34 percent said they were minimally or not concerned

3 Source: http://www.advisenltd.com/wp-content/uploads/cyber-exposures-small-mid-size-businesses-white-paper-2014-10-14.pdf

4 Source: http://www.symantec.com/about/news/release/article.jsp?prid=20121015_01

5 Source: http://www.softwareadvice.com/security/industryview/smb-cybercrime-report-2014/

The total percentage of **concerned small business owners** now reaches 66, nearly inverting the result of the 2012 Symantec survey. Only 27% of respondents said they were extremely confident in the security of sensitive data, with the majority of 52% being only moderately confident. Also, **one third** or respondents answered that they had some form of **data breach insurance** in place. The SMBs seems to be rapidly gaining cyber security awareness.

Government support of Cyber-Security Measures for companies

As costs are high and SMB stand more exposed than ever, government is constantly emphasising the importance of assessing and addressing data breach risk.

In 2009, the National Institute of Standards and Technology outlines the "absolutely necessary" actions that a small business should take to protect its information, systems, and networks[6], the first three being:

• Protect information/systems/networks from damage by viruses, spyware, and other malicious code

•Provide security for your Internet connection

• Install and activate software firewalls on all your business systems

Five years later, the Department of Homeland Security makes the same recommendations specifically addressing SMB: "The cyber adversaries are everywhere, and they prey on the uninformed and the complacent. If you are a business owner, we encourage you to take a few simple steps to improve your company's cybersecurity"[7].

Value of Cyber Security for SMBs

Information security breaches can be especially costly for most SMB. [8]

The Ponemon Institute annual global study on the cost of data breach brings some insightful numbers to the debate:

6 Source: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

7 Source: http://www.dhs.gov/blog/2014/10/24/improving-cybersecurity-small-and-medium-sized-businesses

8 Source: http://public.dhe.ibm.com/common/ssi/ecm/en/sel03027usen/SEL03027USEN.PDF

• The average cost paid for **each lost or stolen record** containing sensitive and confidential information increased more than **9 percent from $136 in 2013 to $145** in 2015.

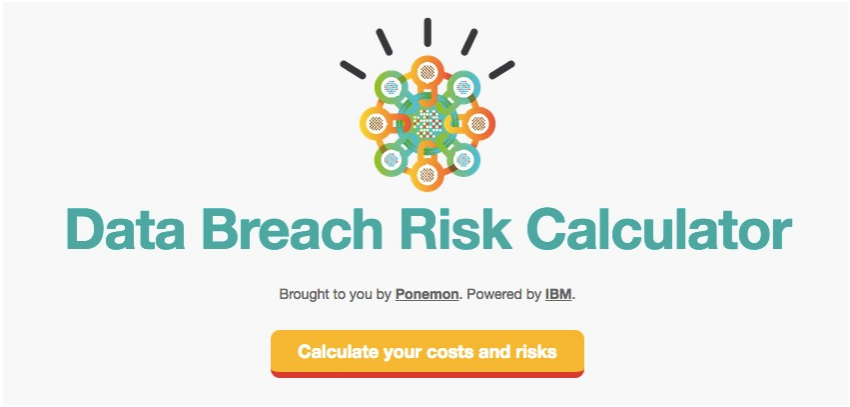
• German and **US companies** had the most costly data breaches ($201 and **$195 per record**, respectively)

• Costs can also vary by industry. **Healthcare, Education, Pharmaceutical** are the **top three industries with the highest per capita cost**. They face a significantly higher per record cost, while others (hospitality, transportation, and retail companies) may face lower than average costs.

• **Malicious or criminal attack stands as a root cause for 42 percent of the security breaches**, being the most frequent cause. It is followed by human error (30%) and system glitch (29%)

• **Malicious or criminal attack** as root cause determined an increased per capita cost of data breach ($159 as compared to 126 for system glitch and 117 for human error)

Companies can calculate the breech amount online using IBM's calculator[9]:



Concern for Cyber-security in SMBs in recent years

Verizon's 2014 data breach investigation report shows interesting cyber victim demographics[10]. According to the final report, more than **75 % of reported data breaches have occurred at small and medium sized organisations[11]** (71% at businesses with 0-100 employees). The threat is real.

9 Source: http://www.ibmcostofdatabreach.com/

10 Source: http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf

And 2014 has certainly determined increased public awareness of security breaches[12]. As a result[13]:

• **65 percent of SMB decision** makers are now more concerned about cybercrime than they were 12 months ago

• **57 percent of SMB decision makers** surveyed plan to **boost IT security** spendings for their businesses in 2015

• Data loss prevention ranks as a **top investment priority** (cited by 25 percent), along with such “core” protections as firewall and anti-malware.

• **Firewall (26%)**, anti-malware, web security and data loss prevention (25 percent each) are top Investment Priorities

Facts are confirmed by recent studies showing small businesses have plans to increase their security budged in recent years[14].

According to the same source, micro-sized small businesses are far less likely to protect against security risks than slightly larger businesses. Only **29% of small businesses with less than 10 employees** say that they are taking any measures, compared to **45% of businesses with 10-19 employees and 45% of those with 20 to 99**. employees.

General **concern** regarding cyber security seems to vary according to the **business size[15]**. For example, targeted cyber attacks represent a concern for:

• 33 % of businesses with 0-9 employees

• 38% of businesses with 10-19 employees

• 42% of businesses with 20-99 employees

11 Source: http://tampabay.issa.org/wp-content/uploads/2014/09/Big-Problems-Scan-Solutions-Verizon-DBIR-John-Linkous.pdf

12 Source: http://www.softwareadvice.com/security/industryview/public-awareness-breaches-2014/

13 Source: http://www.softwareadvice.com/security/industryview/smb-security-report-2014/

14 Source: http://www.csid.com/wp-content/uploads/2014/06/CSID_Whitepaper_SMB2014_FINAL.pdf

15 Source: http://www.csid.com/wp-content/uploads/2014/06/CSID_Whitepaper_SMB2014_FINAL.pdf

The growth of Managed Security Services Market

The Managed Security Services market is expected to experience a dramatic growth in the following years, both as an advancement of the conventional cyber-security maket and as an effect of more and more companies calling for updated security services.

MarketsandMarkets forecasts the Managed Security Services Market is expected to grow from **$14.32 Billion in 2014 to $31.86 Billion in 2019**[16], at a Compound Annual Growth Rate (CAGR) of 17.3% from 2014 to 2019. The researched followed a global industry analysis on Managed Security Services Market, on size, share, growth, trends and forecasts and shown that it could be worth more than $24 billion by 2019, up from roughly $9 billion in 2012.

Research firm AMI also anticipates that **SMB spending on security services will rise over 10% per year** through 2016[17]. **Fortinet** also assumes that the interest of SMB in managed security services has been strongly correlated with the **sharp escalation in regulatory requirements** felt across industry verticals and dramatic increase in security breach notifications in the media.

Gartner Says Worldwide Information Security Spending Will Grow Almost 8% in 2014 as Organisations Become More Threat-Aware[18]. Key aspects of the report:

• Spending on information security will reach $71.1 billion in 2014, an increase of 7.9% over 2013

• Data loss prevention segment recording the fastest growth at 18.9 percent.

• Total information security **spending will grow** a further 8.2 percent in 2015 to reach $76.9 billion

• By 2015, roughly 10% of overall IT security enterprise product capabilities will be **delivered in the cloud**

• More than **30% of security controls** deployed to the small or midsize business (SMB) segment will be **cloud-based by 2015**

• By 2018, more than half of organisations will use security services firms that specialise in data protection, security risk management and security infrastructure management to enhance their security postures.

16 Source: http://www.marketsandmarkets.com/PressReleases/managed-security-services.asp

17 Source: http://www.fortinet.com/sites/default/files/whitepapers/MSSPs_Targeting_SMBs-WP.pdf

18 Source: http://www.gartner.com/newsroom/id/2828722

Technologies and services that secure endpoints, manage identity and access, and provide security and vulnerability management will experience strong growth, according to IDC. Network, messaging and Web security solutions will also be in demand, with **software-as-a-service (SaaS) and security appliances emerging as bright spots**[19].

Conclusion:

Marketing/Sales suggestions to comply when targeting SMBs:

- From the above examples it's clear that Mccann Investigations can customise it's **pricing monthly**, **based on services** provided. Eg: Firewall **charged monthly** and then **up-sell** other services like Content Filtering, Encryption, Data-Backup and Anti-Malware at an additional price.
- Sell **Unified Threat Management** as that is most relevant small businesses
- Market as **Managed Security Services** for larger SME
- Offer **PCI compliance services**, where possible
- Become a regulation compliant business associate
- Make **legal regulation** available on your network
- **Develop specific reports for each sector you wish to target**, to ensure they understand threats
- Reach for **small companies who are government contractors**, as they may be more bound to security regulations.

19 Source: http://www.smallbusinesscomputing.com/News/Security/idc-smbs-to-spend-over-5.6-billion-in-it-security-in-2015.html


MCCANN INVESTIGATIONS
EST. 1984
TOTAL SECURITY SOLUTIONS