

**BBC NEWS****TECHNOLOGY**

6 February 2015 Last updated at 00:18

## Why small firms struggle with cyber security

**By Mark Ward**

Technology correspondent, BBC News

**Keeping cyber thieves at bay is hard. They are busy, well-motivated and well-financed.**

Just one example serves to show just how prolific they are. Every day, come rain or shine, they crank out about 250,000 novel variants of viruses.

Their vigour has helped them steal data from some really big companies, Target, Home Depot and eBay, in the last few months.

And, what is a problem for the big companies is even more acute for the smaller firms. They have an even tougher time keeping the bad guys out.

"They are exposed to many of the same attacks as much larger enterprises, yet they don't have the security expertise and resources available to those larger firms," said Maxim Weinstein, a security advisor at security firm Sophos.

While attacks on the eBays and Sonys of the world make the headlines there's no doubt that smaller firms are getting hit. And getting hit hard.

Figures from Sophos suggest about 30,000 websites a day are being compromised by cyber bad guys - most of those will be the public face of one SME or others.

Becoming a victim of a hack or breach costs smaller firms between £65,000 and £115,000, according to the PWC survey of the worst data breaches among small firms. Those worst hit will suffer up to six breaches a year, PWC suggested, so the total cost could be even higher.

For a smaller firm finding that much cash to clean up after a breach could mean the difference between keeping trading and going bust.

This lack of focus on cyber security is understandable, said Mr Weinstein, as most small and medium-sized enterprises (SMEs) spent most of their time on core commercial activity such as keeping customers happy, seeking out new clients and engaging in all the basic day-to-day admin needed to keep their enterprise afloat.

Worrying about computer security comes a long down their To Do lists, he said.

**Cyber commerce**

But they do need to worry because the nature of commerce in the 21st century means that there are relatively few SMEs that do not make heavy use of technology, said Steven Harrison, lead technologist at IT services firm Exponential-e.

"You do see a knowledge gap," he said "in that you have these smaller companies that are smaller in terms of people and

revenue but they are not smaller in terms of the IT they use."

Ecommerce, websites, apps, smartphones, tablets, social media and cloud services were all now standard ways of doing business in the 21st century, he said.

And, he added, there were some SMEs that were based entirely around technology but that did not make them experts in how to keep their digital business secure.

"There are some businesses that are much more than just users of technology," he said. "They have huge computing requirements as well as massive storage and bandwidth requirements - far more than their head count would suggest."

Either way, he said, everyone is a target and they all need to look externally to security firms for help.

"In the same way they don't run your own bank or accountancy firm they shouldn't run their own security operation," he said adding that SMEs often need help to understand the sheer range of threats arrayed against them.

Everyone is familiar with attempts to penetrate internal networks to steal payment information or customer data records but may be less knowledgeable about invoice fraud, ransomware, malvertising, or even attacks that "scrape" websites with automated tools to steal all the information about prices and products they contain.

#### **Cash question**

And that was where they hit their first problem, he said. How much do they spend? Estimates vary on how much SMEs spend on IT security.

The most recent government figures [published 18 months ago](#) suggest SMEs with 100 or more employees spend about £10,000 per year. The smallest small firms, with less than 20 staff, spend about £200. [Other estimates](#) put the spend at about £30 per employee.

Mr Weinstein from Sophos said SMEs should start with the basics.

This includes anti-virus software, firewalls, spam filters on email gateways and keeping devices up to date. This, he said, would defeat the majority of the low level threats that those busy cyber thieves are churning out.

[Government advice](#) on how SMEs can be safer revolves around a 10 steps programme that emphasises basic, good practice. It's big on those simple steps such as keeping software up to date and applying the widely used software tools that can spot and stop the most prolific threats.

But it also stresses that smaller firms understand more about how they use data and how it flows around their organisation.

This is important, said Greg Hanson from services firm Informatica, because security is no longer about setting up a fortress around your systems, servers and staff to keep the bad guys out. Now, he said, the way data flows between SMEs, their supply chains and customers has made it impossible to maintain the fortress-like security stance.

Having a good sense of where data goes and who uses it can help limit the damage if it goes astray, he said.

"There's a proliferation of data flowing through organisations that really needs to be controlled better," he said.

Having control of that data, knowing its value and where it is going, can help a company guard against it leaking out accidentally and maliciously. For instance, having that control might help a firm spot that a server was accidentally exposed to the net and private information was viewable by anyone.

It can also help SMEs keep an eye on their suppliers and partners to ensure that data is handled appropriately.

And finally, said Mr Harrison from Exponential-e, firms need to put in place a plan for what happens when a breach or security incident does occur.

"It's not a question of if something bad will happen," he said. "It will, but it's all about what they do about it."

## [More Technology stories](#)



[Lenovo offers fix for hidden adware](#)

[\[/news/technology-31565368\]](#)

Chinese computer maker Lenovo offers free software so users can remove hidden software that experts warned made them vulnerable to a cyber-attack.

[US and UK 'hacked Sim card firm'](#)

[\[/news/technology-31545050\]](#)

[Google-backed genetic test approved](#)

[\[/news/technology-31552029\]](#)



Copyright © 2015 BBC. The BBC is not responsible for the content of external sites. [Read more.](#)