Small Business Security Guides

Who's the Bigger Threat? Staff or Cybercriminals

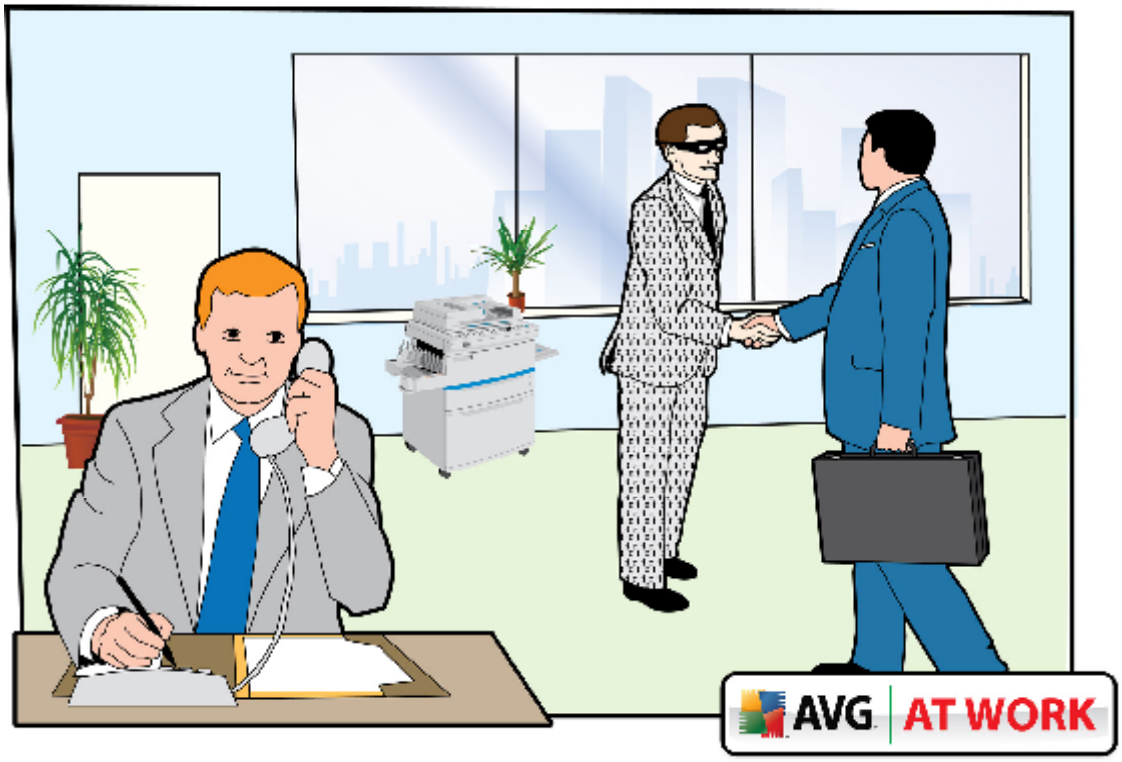
AVG | AT WORK

Who's the bigger threat?
Staff or cybercriminals

Internal staff have traditionally been viewed as a bigger threat to business security than external hackers. Does this still hold true given the increasing sophistication of cybercriminals?

Did You Know?

- A decade ago, viruses and other forms of malware were authored primarily by young, attention-seeking amateur coders
- Research by Verizon suggests seventy-four percent of data breaches are generated by external sources
- Figures cited by the World Economic Forum indicate that online theft alone in 2009 totalled around $1 trillion



Conventional wisdom indicates that the biggest threat to most company's IT networks comes from disgruntled employees rather than shadowy cybercriminals. Staff have access to passwords, and, in the case of the IT department, administrator privileges. What's more, they usually know what they are looking for and what it might be worth to a competitor.

The concept of the so-called "insider threat" has been an enduring one in IT security circles and appears to be based in part on an early-nineties FBI study that concluded that 80 percent of IT security attacks were perpetrated by insiders. However, a lot has changed in twenty years - a millennium in internet time. While once hackers and virus writers were often kids after kicks, today cybercrime has matured to become a big business. Figures cited by the World Economic Forum indicate that online theft alone in 2009 totalled around $1 trillion.

This effective "industrialisation" of cybercrime may well have had an effect on

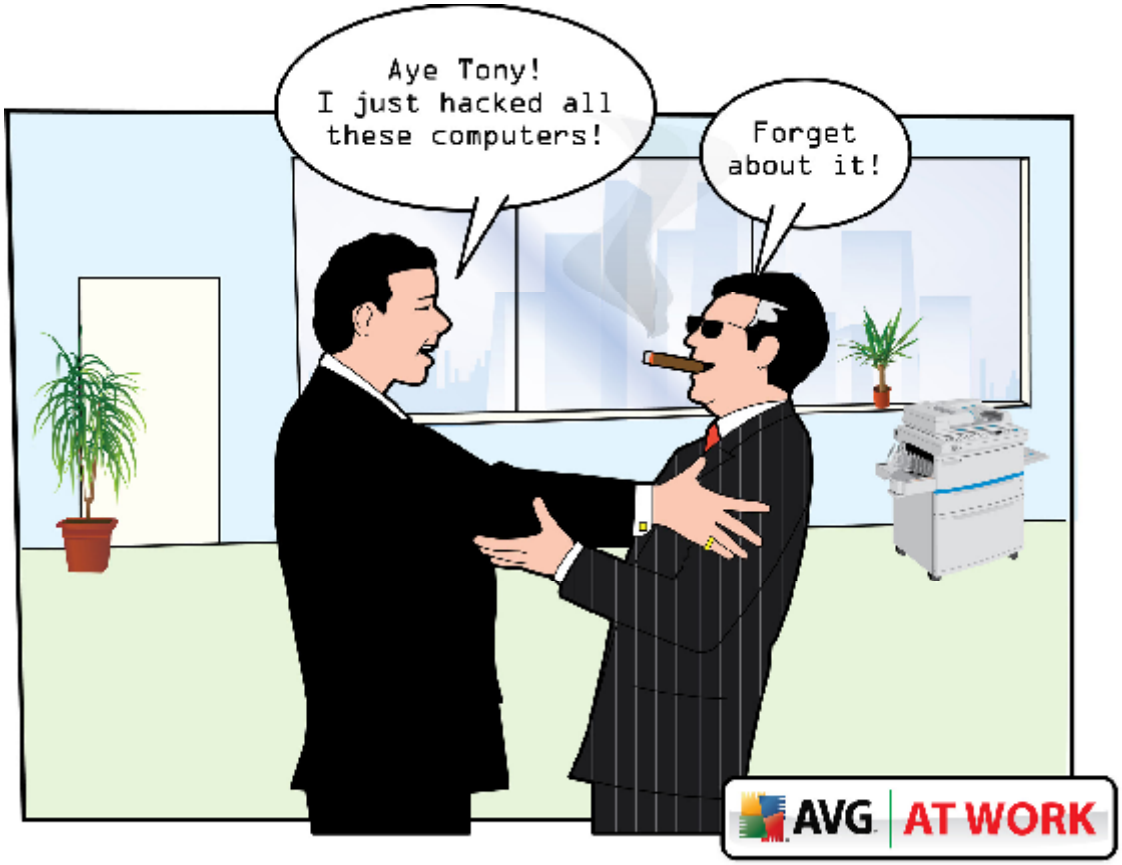
perceptions of whether the "insider threat" should still be the main priority when it comes to IT security. Organised criminal gangs intent on cracking into corporate networks in the same way they might target a bank vault, may seem to be a more pressing threat than the odd-wayward or disgruntled employee. A report from AVG, entitled "Why Traditional Anti-Malware Solutions Are No Longer Enough" explains why companies might want to reconsider where the bulk of their security resources are allocated.

"A decade ago, viruses and other forms of malware were authored primarily by young, attention-seeking amateur coders (script kiddies or script bunnies) seeking to earn notoriety in underground hacker communities," reveals the report and informs that "The security landscape has, however, changed markedly during recent years. Organized criminal gangs realized that there was money to be made from malware and recruited skilled programmers to create malicious programs. These programmes were not intended to cause disruption, but to enable the theft of money or data or both. This led to the creation of an underground economy in which criminals can buy and sell both data and the programs that are used to steal that data."

But while external threats appear to have become more organised with the backing of criminal networks, does this necessarily mean that it has overtaken the dangers posed by disgruntled staff? Experts appear to be divided on the issue; in part due to the definition of what constitutes an internal threat as opposed to an external one. While the nature of cybercrime may have changed over the last twenty years, so has the average business. Companies have become increasingly fragmented and rely increasingly on consultants and outside expertise. Other factors, such as increased mergers and acquisitions, have made the previously stable borders of some large companies become increasingly volatile as they merged with competitors and adopted their staff.

Dawn Cappelli, senior member of the technical staff at Carnegie Mellon University's Computer Emergency Response Team (CERT), recently explained how the organisation has had to tweak its definition of an "insider" to keep pace with business practices. "Our definition of a malicious insider is a current, or former, employee, contractor or business partner," she explained. "We've recently added the business partner aspect of that to the definition because of recent trends that we're seeing."

For its part, CERT, one of the main computer security organisations in the US, still supports the idea that internal threats are where companies should be diverting the majority of their IT security attention. The organisation has a section of its web site "Insider Threat Research" devoted to the issue. "Insiders, by virtue of legitimate access to their organizations' information, systems, and networks, pose a significant risk to employers. Employees experiencing financial problems have found it easy to use the systems they use at work everyday to commit fraud," the organisation claims in a report entitled The "Big Picture" of Insider IT Sabotage.
(www.cert.org/archive/pdf/08tr009.pdf)



But while organisations such as CERT are clear about the threats poised by insiders, other companies believe the increasing sophistication and organisation of cyber-criminals has changed the game irrecoverably. Communications company Verizon clearly believes that external threats are where companies should be focused. The 2009 Verizon Business Data Breach Investigations Report (www.**verizonbusiness**.com/uk/products/security/risk/**databreach**) revealed that seventy-four percent of data breaches resulted from external sources, while 32 percent were linked to business partners. "Only 20 percent were caused by insiders, a finding that may be contrary to certain widely held beliefs," the report stated.

The Verizon report does go onto admit that many internal security breaches go unreported as companies are able to contain the negative publicity that might result from an incident being made public. However, the company still concludes that even with fewer internal incidents being reports, research conducted over several years backs up its argument that external attacks still poise a bigger threat. "Results from 600 incidents over five years make a strong case against the long-abiding and deeply held belief that insiders are behind most breaches," the company states.

But while some security specialists are focused on delineating external threats from internal ones, other experts believe that being too focused on where the attack originated could prove to be a dangerous distraction. "The whole insiders vs. outsiders debate has always been one of semantics more than anything else," security guru Bruce Schneier stated in a blog post. "If you count by attacks, there are a lot more outsider attacks, simply because there are orders of magnitude more outsider attackers. If you count incidents, the numbers tend to get closer: 75 percent vs. 18 percent in this case. And if you count damages, insiders generally come out on top -- mostly because they have a lot more detailed information and can target their attacks better." (http://www.schneier.com/blog/archives/2008/06/it_attacks_insi.html)

Schneier believes that companies would be better off taking a more holistic view of IT security and think in terms of how to safeguard their data and systems from attack no matter where it originates.
"Both insiders and outsiders are security risks, and you have to defend against them both. Trying to rank them isn't all that useful," he states.

Ultimately, it seems that while the danger poised by increasingly sophisticated cybercriminals may have increased over recent years, the increasingly fragmented nature of many companies means that staff, partners and even customers also present a viable concern from so-called insiders. While businesses would benefit from considering the different tactics employed by either group (the cyber-criminal or insiders), the best overall approach is to have a robust and adaptive security strategy in place to keep pace with the fast-evolving nature of IT security.

Robert Gorby


AVG SMB group at:
bit.ly/avglinkedin


Become an AVG Fan at:
facebook.com/avgfree


Read our blogs at:
blogs.avg.com


Follow us at:
twitter.com/
officialAVGnews


Become an AVG
affiliate at:
avg.com/affiliate

Watch our Channel at:
youtube.com/officialAVG

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
Czech Republic
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
United Kingdom
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Deutschland
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com