

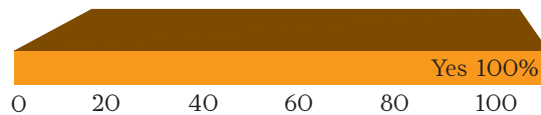
How Secure Is Your Corporate Internet Policy?

No matter how secure your network's IT Policy is, all Internet Security managers face a similar predicament when it comes to answering the following question: what makes your network most vulnerable? The answer, almost every time comes back as, people. You can predict almost everything across your enterprise. Where your firewall might be more effective and how to load balance so that the entire network can operate efficiently.

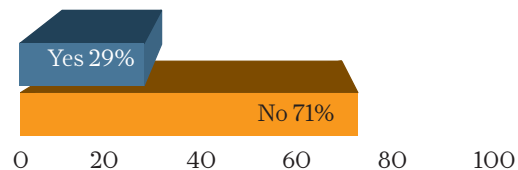
If you can't instill responsibility and ownership or accountability for actions across the workplace, you need to re-think some serious strategy on how to safeguard your network.

But people. What they do is unpredictable and as technology advances, there are more ways to infiltrate IT Policy without really meaning to do so. CSO Pakistan did a random sampling of 50 company employees and asked them a few basic questions, most of which are considered to be bad practice and here's what we got back. We spoke with 50 people of which 14% were Business Development Managers, 14% were CEOs, 14% comprised of Senior Executives and 57% were from the mid-level staff.

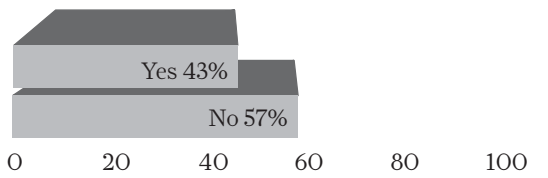
Do you have open access to the internet at your workplace?



Does the network in your workplace use a firewall to restrict internet use?



Have you ever used a free proxy site or application to bypass the restrictions on the network?

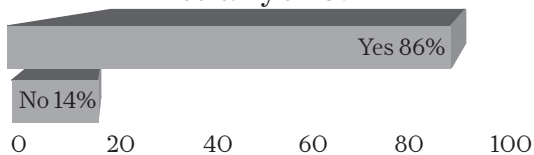


What kind of proxy services have you heard of or used?

Vtunnel	14%
Anonymouse	43%
Proxify	57%
FilterSneak	29%
SlyUser	0%
Other	43%

Population was requested to checkmark more than one option, hence total may be greater than 100%

Have you ever sent an ".exe" file to anyone?



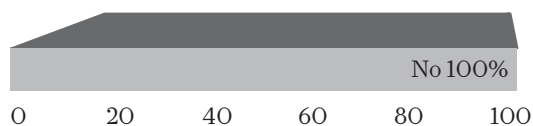
From the mid-sized companies who responded to the survey, 100% said that they had completely open access to internet at their workplace. Only 29% had a firewall implemented on their network, leaving a whopping 71% open to all kinds of vulnerabilities. Thankfully upto 57% have never used a free proxy site or application to bypass any restrictions that might be imposed on their network, however 43% still go to sites which have been blocked by the network administrator. It is this 43% which leaves the rest of the organization more vulnerable, risking to either infect the network by accessing personal email accounts or other sites which may have worms and viruses which can be replicated across the network. Remember - it usually takes only one download or one file to bring down the whole house.

And since people are already trying to chip the network 'byte by byte' from the inside, we thought we might as well ask what they used. 14% had heard of or used a proxy service by the name of Vtunnel. Anonymouse was a bit more popular at 43% of the sample population. 57% had used or heard of Proxify and 43% of the sample population used some other service. We asked people to checkmark as many names as they had heard or used so the numbers do add up to greater than one hundred percent. While the internet is perhaps the best thing to bring enlightenment to mankind, for most things, it seems to have brought a bit too much light.

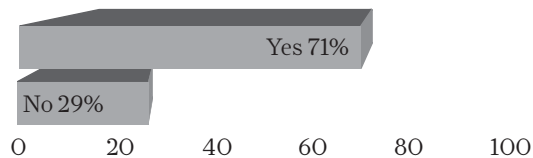
Many organizations have gone ahead to block or severely limit the use of internet access so that searching or free browsing is just not possible. The

Here's a really scary statistic: 86% of the sampled population regularly sends 'dot exe' files to people over email. Even though some webmail services have also started to discourage the delivery of executable files, if you have nobody supervising your network and incoming or outgoing traffic, it becomes a cause for great concern. Here's some good news though! 100% of expressed that they don't download attachments from email addresses they don't recognize. Just to verify and test the respondents, we actually asked the question twice in the survey expecting some discrepancy but then we weren't expecting to deceive our respondents!

Have you ever downloaded an attachment from an email address you may not recognize?



Do you categorize interesting, yet unknown email addresses as SPAM in your email filter?



Discuss:

What are some Internet Security Best Practices that small and medium sized organizations should be following? Do low or no budgets really mean you can never try and increase security? Share your thoughts with us by commenting on the online version of this article or email us at feedback@ciopakistan.com

average employee would then argue that by blocking internet access, the management is also blocking their productivity, which brings us back to the basics: educate the team. At the end of the day, no matter how much you try and block, ban or redirect, there will always be a way to access content.

If you can't instill responsibility and ownership or accountability for actions across the workplace, you need to rethink some serious strategy on how to safeguard your network.

Here's a really scary statistic: 86% of the sampled population regularly sends 'dot exe' files to people over email. Even though some webmail services have also started to discourage the delivery of executable files, if you have nobody supervising your network and incoming or outgoing traffic, it becomes a cause for great concern. Here's some good news though! 100% of expressed that they don't download attachments from email addresses they don't recognize. Just to verify and test the respondents, we actually asked the question twice in the survey expecting some discrepancy but then we weren't expecting to deceive our respondents!

However people sending viruses as attachments are also on the prowl for new and innovative methods. They might

use the prefix "re:" in the email so you think that someone is replying to a previously sent email. Wouldn't the subject line, "re: Your query" look harmless enough for you to click on it and open it up? Subject lines that might pick up a popular trend such as "Long live politics in Pakistan" or other make an emotional appeal, are also more likely to get noticed. And keeping this blackhole in mind, we asked everyone whether they categorize seemingly interesting email subjects from unknown emails into the SPAM filter. 71% exclaimed yes!

People make security a challenge. And because the most effective attacks occur from the inside, every team member who has access to the network, can be turned into a potential threat. Ask any IS Manager and they'll tell you.