

# Internet Security – Safeguarding the Weakest Links

by: YY Ngai, 04/16/2005

<http://www.securitydocs.com/library/3204>

## To the readers:

In my role as a network and server operations manager, I am a frontline Cyber Crime Fighter. In the company, thousands of cyber citizens stand behind me for protection. Attacks by viruses, worms, distributed denial of services (DDOS), and web defacements represent constant threats to me.

My company has been virus free for 3 years, a sign that our virus-fighting strategy has been successful. This paper shares with IT operations managers common worries faced in our cyber age and anxieties felt during outbreaks of Internet threats. Read this tempered with the comforting thought that Internet insecurity also brings job security to IT professionals determined to fight the on-going battle.

This paper approaches Internet securities by looking at the general IT behavior of companies, highlights their most vulnerable areas and shares the corresponding strategies to address them.

## 1. Introduction

We live in the cyber world. Internet has become a defacto network connection for companies. As cyber citizens, we are vulnerable to cyber crimes and cyber wars.

Emailing and web surfing are daily activities of office users, officially and unofficially. Thanks to Internet, communications with people outside the company has made email across the Net rather easy. Information is also readily available on the Net. However, the great ease of accessing information from the Net also exposes us to exploitations from the Net.

This article addresses issues of such exploitations to innocent users. Insider crimes by staff with intention to steal information, mishandling of information due to ignorance, or destroying information out of rage towards boss or employer is not discussed here. Such problems are better addressed by policies, procedures, and user education.

## 2. What are the Internet security issues?

There is a close analogy between the highway and Internet. The highway connects places, Internet connects information. Want to find out about anything under the sun? Go to the Net and click "Search". Even information that is private and confidential is also available on the Net. Shucks, are we vulnerable and exposed!! How did it happen?

Say you buy a fish tank over the Net, pay by credit card, and arrange for the tank to be delivered to your doorsteps. The purchase details, including your credit card number, are sent from your desktop to the online store. The credit card number can be stolen at various points: when you enter it at your desktop, while it was in transit to the online store, or at the online store's database. Information stolen when you enter it at the desktop could be due to a key stroke capture malware which had been installed in the desktop. For theft while on transit over the Net, someone could be "eavesdropping" and therefore managed to capture the data. Theft at the online store is highly possible as it depends on the IT security measures introduced at the other end.

Let us come back to the highway and Internet analogy. Having an Internet connection in the office is like having a highway right outside your office door. The world passes by your door step. On the highway, if a driver discovers a private exit route, he could be tempted to enter and create some mischief at the owner's expense. Similarly, in the internet highway, some script kiddies might stumble upon a loophole in your network, servers, or desktops, target the hole with some worms or Trojan, and Bang!! you have a service downtime on your hands.

Product vendors release security patches weekly, monthly, or quarterly. New-found viruses, loopholes, exploitations of vulnerabilities are sent out by IT security researchers and vendors every now and then. When there is a virus outbreak or spread of new worms, what do you worry about the most? The servers or the desktops? Take a company with thousands of staff and hundreds of servers for example. The chances that one of the thousands desktops get hit is 10 times higher than the hundreds of servers. I would like to say it is 100 times higher given that the servers are managed by IT-savvy folks compared to desktops belonging to office workers who spend a good deal of time using emails and surfing Net.

The desktops users are easy targets. There are many of them, innocent and curious, who enjoy clicking on icons they see on the screens. An outbreak can be sparked off from one of the thousands of desktops in the office, spread to all systems in a few minutes and cripple email communications within the company for hours. Let us take a closer look at the problems these users bring us.

### 3. Protecting the Weakest Link from Attacks by Emails

A typical corporate desktop is Windows-based with MS Office and Internet Browser, with antivirus software installed. That is insufficient to keep virus off. It is not an easy task to manage thousands of desktops out there. Sometimes the antivirus software stops running, sometimes the virus definitions are not updated, sometimes an outbreak spreads so fast that we get hit before the virus definition is available.

There are exceptional cases where virus outbreak starts from someone's Laptop, which was infected with virus while used outside the company. Otherwise, all other viruses and worms enter the company from Internet. The mail server is the first stop of mails from Internet. An antivirus software from a different vendor than that of desktop should be used here for broader virus protection. No two antivirus products and vendors are the same. One product may filter a specific virus better than others, and a vendor may have a specific virus definition file available earlier than others.

Besides matching of virus patterns to pick up viruses, the mail server should have additional filtering to strip off high risk mail attachments. This is an effective zero-day protection to cover the gap when a virus starts to hit the Net till the virus definition is available. Viruses are spread via executable codes, or any codes that users can double click to run it. Such malicious codes come in email attachments. Most company' has email policy to restrict use of emails for official purpose only. So administrators can strip off attachments that are for non-official purpose.

Word, pdf, and zip files are commonly used for sharing official documents. Allow these documents to pass through with virus scanning. Attachments like pictures, images, or screens are usually for personal use. Others like scripts and command files are more likely to be used by IT folks. Strip off these attachments without scanning. This gives you zero-day protection. The IT folks will find other means to share their documents.

### 4. Protecting the Weakest Link from Attacks over Net Surfing

We surf Net everyday. We get lots of information from the Net. Knowingly and unknowingly, we also contribute information to the Net. Knowingly, we sign up for newsletters with our personal particulars. Unknowingly, our userID and passwords, or credit card numbers could be stolen. There are 2 ways information gets stolen:

1. Users enter their accounts, credit card numbers, personal, or sensitive information on some bogus websites.
2. Users click on an icon from a website to download pictures or games. Unknowingly, malware is downloaded to their desktops.

Risks exposed by Net surfing are a result of users' own actions. There is a whole company of users surfing millions of web sites out there. A general path of Net surfing traffic originates from desktops, passes through the Proxy server, Firewall, and out to Internet. Proxy server and Firewall are the control points for net surfing. However, tools and utilities that guard against these threats are less credible than antivirus software. My article in [The Use of Network Intrusion Detection System](#) discusses

this subject.

Ports 80 and 443 are sufficient for office users to surf Net. Do not open Windows RPC ports like 139, 445 unless you have control over what source IPs can access these high risk ports. The RPC ports are favorite ports of worms and Trojans.

User education to raise Internet security awareness is important. Users need to know the pitfalls on the Net.

## **5. Summary**

We discussed the two common office applications; email and Net surfing. Office users are the enablers of virus, worms, Trojans, and other intrusions. They click to open mails, click to visit websites, click on anything they see. Internet is not safe – bring home this message to every of your colleague. It takes everyone's effort to maintain a safe office environment.