Physician Office Readiness for Managing Internet Security Threats

Karim Keshavjee¹, MSc, MD, MBA, CCFP; Nick Pairaudeau², BA; Alisha Bhanji¹

¹InfoClin Inc, Toronto, Ontario, Canada
²DMLink Inc, Toronto, Ontario, Canada

Corresponding Author:
Karim Keshavjee, MSc, MD, MBA, CCFP
President, InfoClin Inc.

Email: karim@infoclin.biz

Abstract

Background: Internet security threats are evolving toward more targeted and focused attacks. Increasingly, organized crime is involved and they are interested in identity theft. A recent report showed an increase of over 140% percent in the number and severity of Internet security threats in the last 6 months of 2005 [1]. These threats include viruses, trojans, spam, spyware, phishing, pharming, intruder and many other ever newer, ever more nefarious threats (malware). Increasing use of the Internet in medical practice is exposing medical clinics to these newer threats. Physicians who use Internet in their practice are at risk for being invaded.

Objectives: Although many have made recommendations about privacy and security practices for medical clinics [2], there are few studies that actually address physician office readiness to handle Internet threats. We sought to understand physician knowledge, perception, readiness and actual security practices to address various Internet related security risks.

Methods: We used questionnaires, site assessments and actual detection of threats using an advanced, monitored Internet security device (ISD), capable of providing real-time detection and management of common Internet threats to study physician practices. 16 physicians in Southern Ontario who use the Internet in their practices were recruited for the 2-month study. They completed pre- and post-study questionnaires. All sites were assessed for presence of firewalls and malware detectors on all workstations. Frequency of updates and scans was also assessed.

Results: 90% of physician had heard of 7 common Internet threats. 70% indicated they are aware of Federal and Provincial privacy legislation and 55% said their practices complied with the legislation. Physicians in the study had an elevated sense of their ability to withstand Internet threats –65% felt safe from most Internet threats and 75% felt satisfied with their current Internet protections. However, physicians in the study were poorly equipped to handle newer threats. Although 90% of physicians had a firewall, none actively managed them. 80% of workstations in the practices studied had a virus checker. Tellingly, only 60% had an updated virus checker and only 40% of workstations had had a scan within the past month. Less than 25% of practices had spyware or spam detectors.

Conclusions: Passive firewalls and infrequently updated virus checkers are poor defenses against determined attackers who are increasingly less likely to be amateurs and students and more likely to be part of organized crime, determined to steal identities and to utilize vulnerable computer networks for spreading spam and viruses. Organizations wishing to increase utilization of technology in community physician offices need to carefully consider the vulnerability of these locations and provide adequate, monitored and managed protection from Internet security threats and regular preventive workstation and network upgrading.

KEYWORDS
Internet; Internet security; virus; spyware; malware; privacy; security; spam

Introduction

Physicians are increasingly sharing patient information and sensitive medical data through electronic networks. Finding and implementing simple, cost effective and sustainable technologies that provide effective security for small physician office environments is necessary.

Internet based threats have been growing substantially over the past years and have increased in number and type. The most recent Symantec Internet Security Threat report (Mar 19, 2006) indicates the largest increase ever recorded of several internet...
threats, including an increase of 142% in viruses and worms during the first six months of 2005 compared to the same period in 2004 [1]. With so much financial activity occurring on-line, it is no surprise that criminal organizations motivated by profit are now more heavily involved than thrill-seeking hackers. These organizations often attempt to perpetrate criminal acts, such as identity theft, extortion, and fraud. Added to this, it takes more time to react to security problems, which can make them harder to deal with. And it’s not only threats that have increased in number. Vulnerabilities in software that allow these attacks have also increased. Figure 1 shows a report from Cert [2] indicating that vulnerabilities have increased significantly in the last 3-4 years.

Figure . Growth of Internet Vulnerabilities in Software from 1995 to 2004

Solo and small group practices (i.e., 1-6 physicians) make up the majority (i.e., >80%) of the total practicing physicians in Canada. Unlike their counterparts in the Hospital or University setting, most have neither the support of an IT department, large IT financial resources, nor the time or expertise to implement a comprehensive IT solution. Our intent in this study was to understand physician practice readiness for new electronic medical record technologies and their understanding of the policies and procedures in place and their ability to comply with current Federal and Provincial privacy legislation.

Methods

A literature review in MEDLINE and EMBASE was compiled from January 2000 to April 2005, using the key-words “Internet security”, “Firewalls”, “Security Networking”, “Privacy & security”, and “Security Information Systems”. Only 3 articles of worth were discovered. Most articles focused on larger institutional or national, state/province privacy and security issues. None tested a security device in a clinical setting.

We installed a managed Internet security device (ISD) from Fortigate in 16 practices in Southern Ontario all of which had high speed internet access. Physicians were asked to fill out a questionnaire on their knowledge and perceptions about Internet threats. Each site was assessed for its current data security practices, including whether servers were kept in secure areas and how often they updated their threat checkers and how often they scanned their computers for various threats. The assessment tool was developed utilizing accepted auditing standards [4,5,6]. Finally, the logs of each ISD was studied over a 2 month period to understand how often the site was at risk and what type of risk it faced.

Results

The following graphs provide some background information on security practices in physician offices in the study.
Most physicians (>70%) in the study felt they were aware of and familiar with the Ontario PHIPA and Federal PIPEDA legislations. More than 50% of them also felt that their practices complied with the new legislation.

Most physicians in the study had some familiarity with common Internet security threats, such as viruses and hackers. Few had heard of zombies – having a computer taken over for fraudulent use.

Physicians in the study appeared to have a realistic idea about the potential damage that could be caused by particular types of threats – including realizing that viruses could be damaging and that spam was mostly a nuisance.
Most physicians feel they are safe from Internet security threats. Over 70% of study physicians agreed to some extent with the statement, “I am very satisfied with the current level of Internet security in my practice.” When asked about their doubts, just under 50% did agree that they sometimes harbored doubts about their security and over 60% agreed that if a threat were to invade their practice, the damage could potentially be catastrophic to their practice; i.e., it could lead to loss of data, business continuity or loss of earnings.

Table. Inventory of Security Practices

<table>
<thead>
<tr>
<th>Security Practice</th>
<th>Number Using (%) N=10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server kept in locked area (N=10)</td>
<td>8 (80)</td>
</tr>
<tr>
<td>Intrusion Detection System (N=16)</td>
<td>0 (0)</td>
</tr>
<tr>
<td>Wireless Connection (N=16)</td>
<td>4 (25)</td>
</tr>
<tr>
<td>Virus Checker (N=35 workstations)</td>
<td>28 (80)</td>
</tr>
<tr>
<td>Recent virus checker scan (N=35)</td>
<td>13 (37.1)</td>
</tr>
<tr>
<td>Firewall (N= 16)</td>
<td>14 (87.5)</td>
</tr>
<tr>
<td>Spyware Checker (N=35)</td>
<td>8 (22.8)</td>
</tr>
<tr>
<td>Recent spyware checker scan (N=35)</td>
<td>2 (5.7)</td>
</tr>
<tr>
<td>Spam Filter (N=35)</td>
<td>13 (37.1)</td>
</tr>
</tbody>
</table>

80% of physicians who had a server did have their server locked in a secure location. However, no practice had an Intrusion Detection System (IDS) and 25% of sites had a wireless network, only one of which was professionally set up. A large majority of our study group had both a firewall and virus checker, thus making them compliant with the Provincial Medical association’s Privacy toolkit. However, most firewalls were set up in factory mode setting, nullifying most of their security benefits. Only 22% and 40% of sites had a spyware checker and spam checker, respectively. Although most computers have a virus checker, less than half of the computers with a virus checker had had a recent (in the last month) scan and less than 10% had had a spyware scan. Although most physicians do not have a spyware checker, the most recent versions of virus checkers do test for spyware.

Activity Detected at the ISD

The major finding from the ISD logs was the heterogeneity of physician use of the Internet and the need for dynamic configuration of threat management. For example, one physician used an ASP-based electronic medical record. Large amounts of data were being transferred through the device on a daily basis. On some days, the device would slow data transfer down dramatically, even though the system was accessing a secure site that probably didn’t need as much security as other sites the physician was visiting.

Another physician used Skype, a popular Internet telephony application, for communicating with friends and colleagues. Large amounts of data were unnecessarily being screened for Internet threats—slowing down applications and user experience. Yet another physician regularly downloaded large files –most of them from safe sites.

More than sixty nine percent of our study group had virus activity that was found and stopped during the research period. A number of these viruses found were resident on physician office computers before the installation of the ISD. Some of these viruses were trying to propagate by sending malicious traffic out of the physician’s computer network. Throughout the duration of the study a plethora of other threats were
detected; these threats originated from various sources including email, webmail, web use and FTP traffic. The ISD detected and stopped both internal and external threats from propagating.

**Physician Time and Resources Spent in Managing Threats**

Physicians in the study spent about 30 minutes on average per month on maintaining and managing Internet security on their computers. They spent on average $112 on virus checkers per year and about $200 on firewall.

We asked about physician willingness to pay in two ways: Free text entry and a structured question that asked them to pick a number from a list. With free text entry, physicians indicated that they would be willing to spend, on average, $55 per month (95% CI $24) for a managed Internet security service. The minimum willingness to spend was about $10 and the maximum was $100, with a median of $50. Physician response to the structured questionnaire shows that they may be willing to pay a slightly higher price of $86 per month (95% CI + $25). The minimum was $75 and the maximum was $200, with a median of $75.

**Discussion**

Physicians have an over-inflated estimation of their Internet security readiness. Although their knowledge is good, security practices in most physician offices was quite poor. Physician offices appear to be like any other small business --viruses and malware are the major Internet security issues. Seven of sixteen sites were infected with viruses at the time the ISD was installed. The ISD helped in two areas. First, it prevented the virus from leaving the network and infecting others and second, it alerted security staff so that the virus could be removed from the infected computers. This reduces the spread of the virus and decreases down time from computers not working as they are designed. Because the doctors in the study did not host services like web and mail servers, there are less intrusion related issues. We did not detect any trends unique to doctors. Most findings followed what is currently going on with the rest of the internet.

**Acknowledgments**

This project was fully funded by Emergis, a Canadian eBusiness company that helps organizations optimize efficiency by conducting business electronically. We would also like to thank OutSource IT for providing some of the ISD implementations and consulting support. The study was conducted by InfoClin, a company that focuses on Electronic Medical Record implementation and Technology based clinical research at the community level.

**Conflicts of Interest**

None declared.

**References**