# MEDICAL DATA RISK EXPOSURE

**Tzveta Dimitrova**

*BULGARIA*
*Technical University Sofia*
*8 Kl. Ohridski*
*Sofia 1000*
*e-mail: tz.dimitrova@gmail.com*

## *Abstract*

*As networks are gradually turning into more intricate and accessible infrastructures, the threat environment is changing dramatically. New security risks are discovered every day in commonly used applications, operating Systems and network components. These are used by hackers and criminals to carry out attacks. With the increased dependency on information technology, the consequences of attacks are becoming increasingly severe. The victims are suffering from losses related to interruption in business, bad publicity and exposure of confidential information.*

*Medical organizations are forced to continuously maintain the protection of their networks. Traditionally, this has been accomplished by creating barriers against attacks by investing in reactive security tools such as firewalls, anti-virus tools and intrusion detection systems. In today's environment these reactive mechanisms simply are not enough. Instead of waiting for attacks to occur, there is a need to take a proactive approach. Only by using proactive security tools that continuously identify security risks, it is possible to effectively manage and reduce the risk exposure.*

*Legislation and compliance with security requirements are also becoming more demanding. The PCI (Payment Card Industry) security standards, Gramm Leach-Bliley act, HIPAA, Sarbanes-Oxley, among others all include requirements for regular testing of network security.*

*This article precents one of the steps in IT security applied in medical centers. This article, however, also points out that healthcare organizations appear to be increasingly vulnerable to exposing our personal health information as measured by the incidence of "reported" data breach incidents.*

## 1. INTRODUCTION

In a paper-based charting environment (where most of the medical records reside nowadays), securing medical data – so-called Protected Health Information, or PHI – is a manual process.

Email communication, however, which flows across public, shared "information highways," is not suitable for PHI transmission, as it is not encrypted – in order to communicate PHI this way, a secure connection must be established. Secure web mail sites have been created which allow electronic transmission of PHI.

Secure websites with medical data have become an integral part of our day-to-daylife. People conduct both their personal and health-related information using these sites. Many consumers purchase medical goods online using sensitive credit card information.

Due to the sensitive nature of these sites, security is a top priority. They all deploy protocols such as SSL and many of them hire security experts to conduct vulnerability assessments.

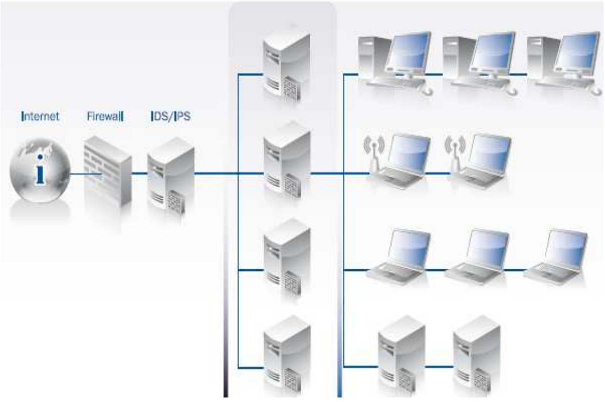

Fig. 1. Network accessable for vulnarabilities

## 2. MEDICAL INFORMATION VULNERABILITIES

When medical information is moved from paper onto an electronic platform, additional vulnerabilities for security breaches (i.e. theft) need to be identified and addressed. When implementing a local, client/server legacy EHR system, there are issues of securing the source of medical information (the server, which is the e-equivalent of the paper chart rack), as well as electronic transmission of data across computer connections. If any PHI is stored locally onto workstations (which may occur, depending on the EHR system being used), then that workstation needs to have locks on it – password access to restart when timed out, as well as the need to have whatever PHI may be stored on the workstation encrypted too. A more significant risk is when the server is broken into and stolen, or local backup data devices are stolen. Physical theft of hardware containing PHI is an area of risk for local client/server EHRs and should be addressed by a policy and security plan at the local office.

## 3. VULNERABILITY ASSESSMENT AND MANAGEMENT

Vulnerability management is a process that can be implemented to make IT environments more secure and to improve an organization's regulatory compliance posture

The vulnerability management process includes these steps:

- Policy definition is the first step and includes defining the desired state for device configurations, user identity and resource access.
- Baseline your environment to identify vulnerabilities and policy compliance.
- Prioritize mitigation activities based on external threat information, internal security posture and asset classification.
- Shield the environment, prior to eliminating the vulnerability, by using desktop and network security tools.
- Mitigate the vulnerability and eliminate the root causes.
- Maintain and continually monitor the environment for deviations from policy and to identify new vulnerabilities.

The technology provided by vulnerability management vendors can be used to automate various aspects of the vulnerability management process. The four main technology categories are:

- Vulnerability assessment.
- Security configuration management and policy compliance.
- IT security risk management.
- Security information and event management (SIEM).

Using automated services is like having a highly skilled security team constantly probing your network to discover vulnerabilities. Identified vulnerabilities are rated and reported together with recommended remedy. The process of correcting identified vulnerabilities is supported by workflow tools for delegating remediation tasks to appropriate administrators. The results can also be compared over time, to monitor trends in risk exposure.

In contrast to manual penetration testing, automated vulnerability scanning is typically performed very frequently. This is important as new vulnerabilities are discovered in a high pace and your risk exposure increases in proportion to elapsed time since the last assessment of your network.

Other advantages of usingnormaly outomated services include:

- Proprietary technology
- 24/7 technical support
- Ease-of-use yet flexibility
- Cross platform support
- Maintains network availability
- Alignment with standards

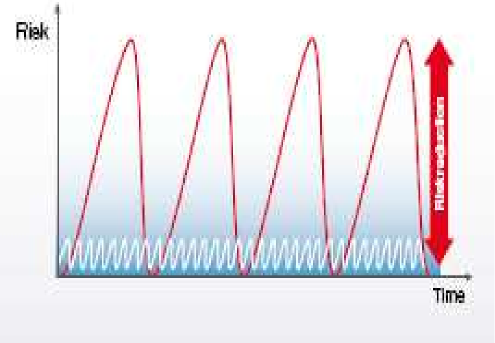

Fig. 2. Schematic risk exposures

## 4. METHODS USED BY CYBER CRIMINALS

You may ask yourself how is it possible for a cyber criminal to store child pornography on your computer without leaving any traces, how someone can get inside your corporate network to get their hands on your intellectual property and how such massive quantities of stolen financial account details, credit card numbers and personal identity information can be available for sale on the Internet? To straighten it out let's start with dividing attacks into two main groups; opportunistic and targeted attacks.

An opportunistic attack is when a cyber criminal targets potential victims randomly in the hope that some of them will be vulnerable to an attack. It is not important for the criminal who the victim is, but rather how many victims there are. For example, a cyber criminal stealing and trading stolen credit card information is likely to take an opportunistic approach as his income is in direct proportion to the number of credit card details he can offer on the underground market. Mass mailing attacks are a typical opportunistic approach where the criminal only expects a low percentage of the targets to be affected.

In a targeted attack, the victim is a specific organization or person. Some possible scenarios could be cyber espionage, hijacking of a website due to political reasons, blackmailing or personal attacks for reasons of revenge. In general it is much harder to protect against a targeted attack, as the attack is tailored to make use of the specific security weaknesses you are exposed to rather than being a generic way of attacking the easiest targets, i.e. the least protected networks.

The traditional way of committing cyber attacks has been to send different types of malware, e.g. computer viruses or Trojan horses, in mass-mailing attacks to potential victims. Because commonly used anti-malware solutions today handle these kinds of opportunistic attack attempts quite well, the "effectiveness" of these kinds of attacks has definitely decreased.

But don't make the mistake of letting this give you a false sense of security. The cyber criminal community is very creative and dynamic in its nature. The methods for exploring the growing number of security weaknesses are constantly evolving. At the same time our network infrastructures are becoming increasingly complex, integrated, and open - which expands the attack surface for cyber criminals.

A very insidious way of committing cybercrime is to turn a legitimate website into a weapon to compromise and control computers that visit the website. This is achieved by injecting malicious code into the website by exploring vulnerabilities in the website architecture. Once the malicious code has been executed on your computer it is under complete control of the criminals, most likely without your knowledge. If your computer is connected to a network, you have now also provided the cyber criminals with an entry point to that entire network. Even worse, you computer can be used for criminal activities such as botnet attacks, where a large number of compromised computers are used as "weapons" by cyber criminals.

For targeted attacks, a very common approach is to hack into an organization's network by making use of security vulnerabilities that the infrastructure is exposed to. Vulnerabilities can be known security weaknesses or misconfigurations of any software or hardware component in the network. In fact, there are tens of thousands of publicly known vulnerabilities, with numerous new vulnerabilities being discovered every day.

Hacking into networks may sound like something only a small community of very skilled technical people is involved in. However, that is no longer true since several different hacking tools are available for free or for sale in the underground communities.

The most popular hacking tools include:

***Exploits*** – A small piece of code that explores specific vulnerabilities. This can be everything from exploits making use of general vulnerabilities in web browsers to exploits targeting site specific vulnerabilities on financial sites.

***Autorooters*** – A tool that scans any specified network range for vulnerabilities. Found vulnerabilities are automatically explored by executing an exploit on the compromised computer providing the attacker with complete control of the computer. The autorooters then remove all traces of the intrusion by cleaning log files. According to Symantec, autorooters are available from $40 with an average price of $70.

The characteristics of a hacker have changed quite dramatically over the last few decades. The nice high school student in WarGames is no longer a good representative of today's heavy cyber criminals that are the brains behind the organized and economically devastating crimes being carried out today. The availability of easy-to-use tools for performing cyber-crime activities has definitely contributed to this development, luring in potential attackers all over the world and bringing cyber-crime to a completely new level.

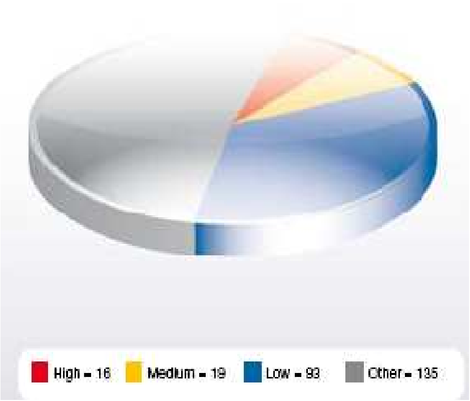

Fig. 3. Medical data risk exposure overview

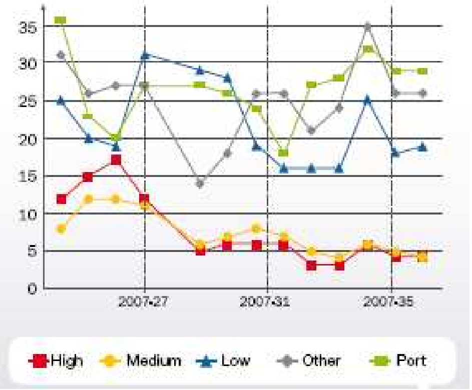

Fig. 4. Trend in risk exposure overview – weekly overview

## 5. CONCLUSION

As one can see, when health information moves from paper to local electronic systems, and then to hosted "cloud"-based systems, the risk of security breaches is actually *reduced*, provided that the vendors and systems utilized conform to specified standards covered by vulnerability management.

To summarize, cyber-crime has turned into a well-developed underground market of massive magnitudes. Attack methods are getting more sophisticated every day and organizations of all sizes are potential targets. So what can be done to protect your valuable assets?

First of all, it is important to take an overall approach to IT security. The chain is not stronger than the weakest link so it is crucial not to lose sight of the big picture. At the same time, we can conclude that most organizations have already implemented anti-malware software, firewalls and other reactive measures. Unfortunately, that is no longer enough. With today's complex and open network infrastructures combined with a true explosion in security vulnerabilities in commonly used operating systems, applications, and hardware components a more proactive approach is needed.

In order to compromise a website or a network, cyber criminals, or the tools they are using, search for vulnerabilities to exploit. When visiting a website on which malicious code has been implanted, you are at greater risk of infection if your web browser has unknown vulnerabilities that can be exploited. Today, actively managing and eliminating vulnerabilities in order to reduce your risk exposure to an acceptable level is absolutely key. As new vulnerabilities are discovered at such a rapid pace, an automated approach that provides the ability to assess the network on a regular basis is the natural starting point.

## References

[1] L. Cranor, P. Guduru, and M. Arjula. User interfaces for privacy agents. ACM Transactions on Computer Human Interaction, 12(2):135–178, 2006.

[2] R. de Paula and et. al. Two experiences designing for effective security. In SOUPS '05: Proceedings of the second symposium on Usable privacy and security, New York, NY, USA, 2005. ACM.

[3] R. Dhamija, J. Tygar, and M. Hearst. Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2006.

[4] J. S. Downs, M. B. Holbrook, and L. F. Cranor. Decision strategies and susceptibility to phishing. In SOUPS '06: Proceedings of the second symposium on Usable privacy and security, New York, NY, USA, 2006. ACM.

[5] D. Florencio and B. C. Cormac Herley. Do strong web passwords accomplish anything? In Proceedings of the USENIX Workshop on Hot Topics in Security (HotSec), 2007.

[6] L. Freed. State of customer satisfaction with online banking, forsee results/forbes.com, April 2007.

*The paper is published with the financial support of the National Science Fund, Contr. № ДО 02-211/08.*