SPECIAL REPORT

Cybercrimes Pose Growing Threat to Medical Devices

Axel Wirth

Securing medical devices against cyberattacks or malware outbreaks and safeguarding protected health information (PHI) stored on devices or exchanged between a device and the provider’s network is a growing challenge for clinical engineers and hospital information technology (IT) professionals. This article will analyze two general trends with regard to their impact on a medical device security strategy: first, the increased exposure and vulnerability through the growing number of devices connected to a network, and, second, the changes in the cyberthreat landscape. Threats are becoming more prevalent, complex, and sophisticated, and are being driven by a cybercrime culture that is moving away from sensationalism to targeted attacks based on financial motivation.

A medical device, in the context of this article, is any network-connected system used in patient care in a hospital, private office, home, or other healthcare setting, and which, due to its usage model, operating system, configuration, and network communications, can be exposed to cyberthreats—for example, through a permanent or intermittent network connection or through “sneakernet,” a term that describes the transfer of electronic information by physical means, such as a USB or universal serial bus, device.

Why are Medical Devices Difficult to Protect?
We are witnessing a transformation of the healthcare industry and specifically the country’s healthcare IT infrastructure. The American Recovery and Reinvestment Act (ARRA) of 2009 and the Health Information Technology for Economic and Clinical Health (HITECH) Act encourage healthcare providers to implement electronic medical record (EMR) systems, upgrade existing IT infrastructure, and automate workflows and processes, all with the goal of reducing healthcare costs and medical errors, improving quality of care, and increasing workflow efficiency. This transition includes increased integration of medical devices with enterprise IT systems, which enables the automatic updating of patient data (such as identification) or treatment information (such as dosage) to the device, as well as the delivery of monitoring or diagnostic data (such as vital signs) to the EMR or other IT system.

Traditionally, medical devices have been used in a stand-alone mode or have had limited network connec-

Vulnerability Issues

- Networked medical devices are exposed to the same cyberthreats as IT systems, yet are much more difficult to protect and remediate.
- Medical device characteristics, like regulatory oversight and long product life cycles, make them difficult to protect against cyberattacks.
- With close to 2.9 million new virus signatures released in 2009, it can be estimated that as much new malware was generated in that year alone as in the entire history of computing.
- Hackers have turned from fame to fortune and it is estimated that the business of organized cybercrime is now exceeding illegal drug trafficking.
- With new and more sophisticated attack vectors emerging, it is no longer sufficient to rely on the larger network to protect medical devices. In fact, a new paradigm has evolved where a medical device can become the entry point for an attack and the weak link in the larger enterprise security posture.
- Protecting medical devices against cyberthreats requires a comprehensive approach of securing the device itself as well as the larger network.
itivity, typically to a proprietary subnet of similar devices (e.g., a patient monitoring network). However, economic pressures, the increasing use of IT, and the desire to improve staff efficiency and quality of care have led to a usage model where more devices are integrated with the larger hospital IT infrastructure. Attractive price points and lower maintenance costs make standard Internet protocol (IP) networks the technology of choice. Similarly, device manufacturers increasingly utilize commercial technologies, standard operating systems, or other off-the-shelf software components, as well as commercial central processing unit (CPU) platforms.

Although the economic benefit of this approach is clear, it has introduced vulnerabilities and is exposing medical devices to common cyber threats. This problem is compounded by the fact that the number of cyber threats, along with their sophistication, is increasing.

Self-replicating malware is of particular concern in the medical device environment. With “worms” being a common and increasing occurrence, they are a serious threat and often open the door for subsequent outbreaks or infiltration of the larger enterprise. Figure 1 shows the top 10 most prevalent malware strains with download capability.

Particularly troubling for the medical device environment is the increase in worm-like threats over previous years as seen in Figure 2.

Medical equipment is more difficult to protect than standard IT infrastructures for several reasons:

- Medical device design and distribution is tightly regulated. In the United States, the authority over medical device distribution lies with the Food and Drug Administration (FDA), which stipulates that the responsibility for the approved configuration of a device lies with the manufacturer of record. Consequently, the end user of the equipment—for example the hospital—has no access to the device’s software environment and cannot install secondary cybersecurity measures. Any upgrade or change to configuration, whether it is software patches or security measures, typically needs to be approved by the manufacturer, which delays the deployment of security-relevant upgrades.

- Characteristics of medical device life cycles negatively impact the ability to secure them by traditional means. Typically, medical devices have a long life and often use older generation operating systems, many of which are not supported or updated anymore. Further, due to regulatory oversight, patches and upgrades require manufac-

---

**Figure 1. Top 10 Trojans and Worms With Download Capability in 2009**
turer validation, which unfortunately delays their availability. Also, when patches and upgrades are applied, they may require complex installation procedures and acceptance testing. As a result, many devices are behind in operating system patches or other critical upgrades needed to address vulnerabilities associated with off-the-shelf software components.

- Driven by cost and design restrictions, available memory space is often limited. This has led many manufacturers to use customized or scaled-back versions of standard operating systems. From a design perspective, this is a perfectly reasonable approach; however, as a result, it becomes difficult to apply software patches or to utilize common security software solutions.

- Use of the latest and greatest software platform is typically not a major design objective for the manufacturer. To use a simple example, whether an electrocardiogram (ECG) system is based on a Windows 7 or a Windows NT platform makes little difference to the end user and the diagnostic results. It does, however, make significant difference from a cybersecurity perspective.

- Many healthcare providers tend to standardize with one manufacturer and model for a specific type of device. This is, of course, reasonable, awarding better economies of scale and reducing the complexities associated with device maintenance. From a cybersecurity perspective, however, it creates a homogeneous environment with a common security weakness, thus enabling any type of outbreak to proliferate rapidly among similar systems.

Anecdotal evidence confirms that we should be concerned: Conficker, a computer worm, forced one hospital chain to shut down the majority of its medication cabinets and dispense medications manually. In another reported case, a virus outbreak shut down the entire interventional cardiology infrastructure, requiring the diversion of all emergency patients to other hospitals.

### Risk Considerations

Devices may be affected in functionality, performance, or reliability, all of which can negatively impact diagnosis, delivery of medication, therapy, or other aspects of patient care. The most obvious risk with a compromised medical device is the potential to harm, even kill, a patient.

Healthcare organizations need to be concerned about:

- The security of the device itself. A cyberattack or malware outbreak can compromise a device’s operation or performance. Device architecture, communication channels, and integration with the larger network are key considerations when assessing the risk to the device.

- Privacy. The privacy risk of a specific device needs to be evaluated based on several factors: the type of PHI data stored (e.g., is it identifiable data?), the amount of data stored (e.g., does it pertain to one medical device), and the extent to which it can be accessed or shared.

---

Figure 2. Prevalence of Malicious Code Types by Potential Infections

![Figure 2. Prevalence of Malicious Code Types by Potential Infections](image-url)
individual or several patients?), and whether the data is persistent. Healthcare providers should request a manufacturer disclosure statement (MDS) from the manufacturer, which documents the patient data and associated privacy risk of a given device. MDS is a standard established by the National Electrical Manufacturers Association.7

- The security risk to the larger enterprise. Any system or device on the provider’s network with insufficient protection or exposed vulnerabilities, such as an insufficient software patch level, is at risk of being exploited and can become an entry point for an attack on the broader network. Any insufficiently protected medical device is a risk factor to the security of the entire enterprise. In other words, an enterprise is only as secure as its weakest component.

Of these three scenarios, security of the device itself should be the primary concern as any event may directly affect patient care and, in an extreme case, could even lead to death. But as providers develop a security strategy, they also need to be aware of the risk that an insufficiently protected device poses to the larger enterprise.

Privacy of PHI on a device would only be a major concern if it can lead to disclosure, intentional or otherwise, or if the device contains information that could be used for identity theft. Examples of unintentional disclosure include loaner devices being returned or a device being sent in for repair without removing the PHI stored on it. Also, we need to be aware that the exchange of devices with manufacturers or leasing services is a potential risk factor for introducing malware infections.

A Changing World of Cybercrime
We are witnessing significant shifts in the cyberthreat landscape and underground economy. These trends need to be understood and taken into consideration when laying out an enterprise security strategy. Data stored in medical devices may be of less interest to a cybercriminal since the information contained in the device is less valuable to an identity thief, unlike the information in an EMR or financial system. Although “hacking” of medical devices has been demonstrated,4 I’m not aware of any case of intentional penetration of a medical device with the goal to obtain PHI or manipulate the functionality of the device. However, this is certainly not beyond the realm of possibility5 and should be included in a comprehensive risk management strategy.

Because medical devices are difficult to protect and patch, they can very quickly become an unintended casualty during a cyberattack or threat outbreak. In this day and age, the problems around securing medical devices are more serious than ever. Trends in cybercrime and the underground economy have changed the landscape, and it is very troubling. Hackers and cybercriminals have changed from individuals motivated by publicity and the technical challenge to a “business” driven by organized crime and highly sophisticated organizations looking for financial gains. In fact, the general consensus is that cybercrime has now surpassed illegal drug trafficking as a criminal moneymaker.10 As a result, we now see well-targeted and well-executed attack strategies, and a much more complex and concerning risk scenario. The sheer volume of malware is growing exponentially. In 2009, Symantec released a total of 2.9 million new virus signatures, which is a 71% increase over 2008.2 This means that as much new malware was developed in 2009 alone as in the entire history of computing (Figure 3).

In recent times, the number of threats has roughly doubled every year, and there is no indication that this trend will ease. To break this down into something more tangible, in 2003 Symantec, as one of the leading security companies in the world, produced, on average, five new virus signatures per day. Now, Symantec produces tens of thousands of new virus signatures on a single day. Unfortunately, many medical devices in use today were designed based on the security paradigm of several years back.

Similarly, sampling and estimates suggest that we now see more illegal code being produced than legitimate software applications.

- Today’s cybercriminals are no longer motivated by the desire for fame and the “big splash.” In fact, we are seeing just the opposite; attacks are stealthier and increasingly difficult to discover. Attackers use strategies that slowly penetrate IT infrastructures and take their time to find the most valuable assets (or do the most possible damage, if that is their motivation). For example, Symantec estimates that one in about 200 computers in Western countries are part of a “botnet”—a network of software agents running automatically—with the larger ones reaching more than one million computers, actively and unknowingly to their owners contributing to the distribution of spam and malware.11

- Malware production is changing and cybercrimi-
nals now use automated processes to generate new malware strains and variations in rapid succession, enabling them to attack only a few select victims with new strains. Malware authors understand how to build code, which is difficult to detect—it may even use encrypted communication to receive commands and updates from a remote server—and has a minimal footprint, using, for example, standard operating system libraries to reduce size of the malicious code. Tools to generate viruses and cookbooks on how to build certain exploits are readily available on the Internet. Instead of malware which spreads rapidly to millions of computers, we now see microdistribution of code affecting a small number of machines or targeting a specific environment. The obscurity and variability (including self-morphing capability or servers automatically generating variances) of malware is rapidly changing how organizations need to protect their IT infrastructures.

- We also see a resurfacing of old attack vectors. For the past few years, the main penetration route has been the network itself, for example, web-distributed attacks and e-mail. However, the popularity of high-capacity storage devices has opened up a new distribution path similar to the “sneakernet” distribution via floppy disk we used to see in the past. There are several known cases of Conficker—also referred to as Downup, Downadup—outbreaks on medical devices, the most likely cause being introduction by USB memory sticks used for maintenance purposes.

- Organizations need to watch for embedded attack vectors. Many systems contain software of unknown origin, and there have been documented cases of malicious code being included within the software itself. For example, malware has been found on storage media used for distribution of legitimate software, digital picture frames (from which it can be transferred to the enterprise network via USB), or the like.

Protection Strategies
In light of the trends in cybercrime, it is increasingly important to develop a comprehensive security strategy and be vigilant about the changing threat landscape. Only a well thought-out and enterprise-wide approach will protect medical devices, and, vice-versa, a well-protected medical device is essential to the security posture of the larger enterprise. Information and advice on the topic are provided for by the federal government or cybersecurity specialists.

The complexity of the problem clearly requires that all stakeholders—IT departments, clinical engineers, device manufacturers, security specialists, industry organizations, and regulating bodies—work hand-in-hand to enable protection of our hospital networks and patients’ lives.

Based on cyberthreat trends, simple point protection is no longer sufficient. A comprehensive security strategy requires the protection of the perimeter as well as the information and systems located within the perimeter. Here are some key points to consider in securing medical devices:
Antivirus (AV)—Any protection strategy relying on AV alone is not capable of protecting complex infrastructures against today’s sophisticated threats. Although AV is an essential piece of a broader enterprise security strategy, its usefulness for medical devices is limited. Hospitals have no access to most medical devices due to the manufacturer’s control of system configuration. Further, AV software is required to be actively managed, including regular updates of virus definitions. To adapt to evolving threats, sometimes even architectural changes are needed. This is a general challenge, specifically for devices with intermittent network connection. Therefore, not impacting performance or functionality over the device’s lifetime cannot be guaranteed with an AV-based approach.

Also, many medical devices have limitations in computing power or memory space and therefore are not able to run traditional AV software without impacting system performance.

Finally, with any antivirus technology, there is always the risk of a false positive, which for a life-supporting device can lead to a critical, life-threatening situation. However, the limitations of AV should not be generalized and there may be cases where a well-designed antivirus approach is the solution of choice for a specific medical device scenario and especially for the IT infrastructure complementing the actual device, i.e., servers and workstations.

Host Intrusion Detection and Prevention Systems (HIDS/HIPS)—These technologies are based on managing a known behavior of a system and disallowing any unknown behavior. Basically, a given system’s behavior is locked down by “whitelisting” and controlling all known processes, communication, system configuration (like registries)—allowing for a varying degree of tightening of controls all the way to a total lockdown. HIDS/HIPS have very light footprints and are an excellent solution for a single-purpose system, like a medical device. Further, HIDS/HIPS can be deployed in a managed and unmanaged format, which makes them a good choice for medical device protection. Because of their unique protection approach, HIDS/HIPS protect even against “zero day attacks” (i.e., unknown malware), and ease the pressure on product life cycle and the need to update due to security issues.

Access Control—As previously mentioned, introduction of malware to a device can happen via network and non-network vectors. Therefore, it is imperative to understand and control all access paths to the device, including administrator accounts, USB ports, and even wireless communication. For example, administrator accounts should never use the manufacturer’s or operating system’s default user name/password; USB port access should be limited to approved and secure devices; and all transmission of critical data or access to device programming should be encrypted.

Boot Consistency Check—Another technology used to protect systems from being infected is to check its boot behavior against a known good behavior. Although capable of detecting exploits utilizing boot-up vulnerabilities, this method is limited in effectiveness since many medical devices may not be rebooted on a regular basis.

Network Segregation—Network separation via a virtual local area network (VLAN), demilitarized zone (DMZ), or other technologies—as, for example, recommended by the Department of Veteran Affairs,15 can help avoid the spread of infections and contain the damage of an outbreak. However, it should only be considered a complementary method as it does not effectively protect the individually networked segments. Further, these complex systems are difficult to maintain over time and coverage gaps may develop.

Firewalls—The use of network firewalls can help reduce the spread and impact of virus/worm infections and protect a network or segments of networks. External firewalls placed in front of the device can be used as a point solution to protect expensive or critical medical devices from network threats, but, in many cases, their cost makes them a less desirable choice as a general protection approach.

Network Scanning—While AV on a device may not be practical, it remains the most effective way to find threats on a machine or in a network once a penetration has occurred. The use of network-based scanning technologies is a good practice for making sure that machines are free of threats. These types of scans can be applied against the entire network or against specific devices when, for example, they return from repair.
SPECIAL REPORT
Cybercrimes Pose Growing Threat to Medical Devices

• **Asset Management**—It is essential that all network-connected systems are known with regards to their existence and configuration and are managed as part of an asset management database. Automated tools to discover network assets and their configuration are available. Considering that healthcare providers may have tens of thousands of medical devices, the use of these automated systems is required to achieve a sufficient level of granularity and accuracy.

Today, we can automate the discovery of IT properties of a device, such as its operating system, IP address, key software components, etc. But to maximize the benefit of automated asset management, for example to manage device-specific maintenance or error messages, common standards must be established. See the work being done by the Integrating the Healthcare Enterprise Patient Care Device (IHE PCD) working group, specifically the “Device Connectivity Technical Note TN 905.” As an additional benefit, these types of inventory and network discovery systems can be used to track and manage the non-IT aspects of a device, such as the maintenance or disinfection schedule.

• **Configuration and Patch Management**—Related to asset management and a key aspect of any security strategy is the need to determine the security posture of any network-connected device and its level of cyberprotection, along with its software patch level and system configuration. As a protective measure, device software and especially the operating system should be maintained at the latest revision level. Using Conficker as an example, this virus exploited a specific operating system vulnerability and affected organizations that did not deploy the required patch. Even though this virus was not targeting medical devices specifically, it has been quite prevalent and proves the point that only a well-managed system can be a secure system.

However, the fully automatic distribution of upgrades and patches—a common practice in the standard IT environment—is difficult to implement for medical devices. Consider, for example, the problem of upgrade timing, system reboot, or required acceptance test after an upgrade. But once we have discovered device version, patch level, and configuration, we can mitigate any discovered vulnerability, even if this requires manufacturer intervention or manual upgrades.

• **Process Management**—The need to establish reliable processes to manage the medical device life cycle goes hand in hand with asset and configuration management. Starting as early as the purchase (e.g., include a MDS² requirement in the contract), through device acceptance, installation, user training, maintenance, and end of life (e.g., erase all PHI), the use of automated process management tools will increase the reliability and reduce the risk associated with managing the device lifecycle.

• **Security Monitoring**—In an ideal IT environment, we not only manage assets and their configuration, we should also monitor the security events generated by all devices on the network. For example, automatically log and alert a detected malware outbreak or issue a response to failed log-in attempts. Security Information Management (SIM) systems automatically monitor, correlate, and filter all security events provided by the systems in an

---

**What’s What in Malware?**

**Virus:** A piece of self-replicating code that appends itself to a program file or a sector of a disk.

**Trojan:** A program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can obtain control and do its chosen form of damage.

**Worm:** A program that duplicates itself from one directory, drive, computer, or network to another through electronic communication or local area networks.

**Backdoor:** A method of bypassing normal authentication, securing remote access to a computer and data while attempting to remain undetected.

**Rootkit:** Techniques to allow concealment by modifying the host operating system so that the malware is hidden from the user or removal tools.

**Spyware:** A type of malware that can be installed on computers with the purpose of collecting information about users without their knowledge.

**Botnet:** Network of software agents (bots or robots) that run autonomously and automatically, most commonly for malicious purposes, but it can also refer to a network of computers using legit distributed computing software.
IT infrastructure—servers, endpoints, routers, firewalls—as well as network-connected medical devices. In a complex network environment, as we find in our hospitals today, automatic monitoring systems alert us to relevant events and allow us to be proactive in mitigating potential cybersecurity threats.

- **Education**—Organizations should never forget the importance of user education as part of a provider’s security strategy. This includes technical staff (IT and CE) as well as system users. Employees need to be aware of the risks and how their behavior—for example, surfing the web or using personal USB devices within an IT environment—can expose the organization to additional risk.

It would be impractical to implement all of these protection and detection measures, but based on the specific risk management approach taken, a complementary set of several methods is required in order to provide comprehensive protection against today’s complex cyber threats.

General guidelines for the management of medical devices in a healthcare network are provided via the IEC 80001-1 standard, *Application of Risk Management for IT-networks Incorporating Medical Devices*.19

**Conclusion**

The increasing volume, complexity, obscurity, and sophistication of cyberthreats exposes medical devices to a growing risk. Device malfunction can impact diagnosis, patient care, and even lives. Only a comprehensive, enterprise-wide and multi-layer security strategy provides the appropriate level of protection against today’s threat landscape. Medical devices can be effectively protected by managing their behavior and software processes; complementary strategies can be applied to the network environment.

Protecting the nation’s healthcare delivery system is a mission of national importance. Whether the attacks are driven by financial interest or political motivation, the national healthcare delivery systems is at no less risk of a cyberattack as any other key infrastructures.20

Providers, manufacturers, security experts, and industry organizations need to work together to successfully protect our increasingly integrated healthcare system, especially since the underground economy has identified healthcare as a softer target than other industries. In fact, looking at one specific indicator, the healthcare industry is now in second place in the number of data breaches.2 Even though the number of exposed identities is relatively low, the resulting fraud is causing significant financial harm to our healthcare system.21

**References**

SPECIAL REPORT
Cybercrimes Pose Growing Threat to Medical Devices


