
0100101100
0100101100
0100101100
0100101100
0100101100

Your Data is Valuable; Can You Protect it From CYBER THREATS?

By Kerri Wachter
Staff Writer

"We haven't had a cyberattack, so we don't need to worry about data security."

"We see hundreds of cyberattacks every day. We're analyzing them and we're stopping them."

Blood centers can suffer from at least two common mindsets when it comes to data security: They can think they are too small and/or their data is not valuable enough to attract cyber criminals OR that they are on top of the problem and it cannot happen to them. Wrong.

The cyberattack that hit the United Kingdom's National Health System (NHS) in May 2017 made headlines around the world. The "WannaCry" virus behind the attack affected more than 200,000 computers in more than 100 countries[1]. The virus affected more than one-third of the 236 NHS trusts in England and 595 general practitioner (GP) practices[2]. Patient appointments and procedures were cancelled by the thousands, and emergency patients were rerouted in five areas to other emergency departments not infected by the malicious virus. While NHS reported that no patient data was stolen or otherwise compromised, the scale of the incident raised questions worldwide about the security of health care information.

The sheer number of attempts — through phishing emails, infected websites and outside devices — make it very likely that an organization will fall victim to a cyberattack — if it has not already. It can happen to an organization of any size. Scarier still, you may not even know that you have been hit.

Your money or your life

What is it that makes blood banks an enticing target for cyber criminals? It turns out that the kind of information contained in health care records can be much more attractive to certain criminals than even financial information. "That data is worth a lot of money," according to Mike Simon, president and CEO of CryptoniteNXT, a company that provides Moving Target Cyber Defense. "In fact, health data has a premium on the black market. Stealing the records of donors is worth a lot of money to 'bad actors.'"

Michele Scaggiante, vice president and chief information officer (CIO) of New York Blood Center echoed this. "Health care is becoming more and more of a target for a variety of reasons. Health care information, especially medical records and patient data, is very valuable to criminals. There is more value to them in attacking health care organizations than financial institutions sometimes."

It is the breadth and depth of data in digital health records that make them so attractive. "The amount

of data that exists in a health record far exceeds that of financial records. You can 'copycat' a person much easier with her health record — much easier than with a financial record," Simon said.

It is not just the value of health care records that makes blood banks an attractive target. The blood supply is a valuable national resource, making it vulnerable to bad actors on an international scale. A nation-state could infect a blood bank's computer network and wait to activate the program until there is an urgent need for blood. The malware could then be used to shut down any activities at a specific location or in an entire system.

Cybercrime 101

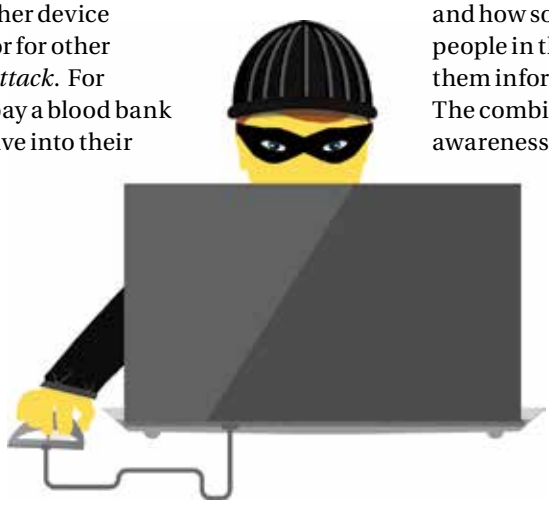
Bad actors can attack your organization in several ways. NHS was the target of a *ransomware attack* — a malicious computer virus hijacked their systems (and the information contained within them). The hacker demanded a ransom to "unlock" their systems.

There are several ways for a system to be compromised by a virus or other malware.

Phishing is a relatively simple, low-cost way to get into an organization's computer network, according to Scaggiante. It can take the form of a legitimate-looking email that appears to come from an executive or another employee within an organization. This approach can be used to obtain usernames and passwords or to install malicious software via a link in the email. Both allow the bad actor access to systems and information.

Websites can pose dangers, as well. Users can visit a website — and it doesn't necessarily have to be a malicious website — where malware automatically downloads onto their computer. "It could be a website infected with an advertiser that does an automatic download [of malware] — without the user even clicking on it," said Simon. This is known as a *drive-by* download.

It is also possible for someone inside the organization to load malware into the system with a simple thumb drive or other device — in exchange for money or for other reasons. This is an *inside attack*. For example, someone could pay a blood bank employee to plug a USB drive into their computer — allowing malware to enter and propagate into the system, according to Simon.



"There are two network weaknesses that the ransomware in the NHS scenario were looking to exploit — and these are very common to a blood bank scenario — the ability to *laterally move* and *scan*," he said.

Lateral movement means that malware can move from your computer, printer, mobile or Internet of Things (IoT) device to other devices on the same network by stealing credentials or by monitoring the communication between these devices. It is a means of quickly expanding the attack from the initially infected computer or device throughout your entire network.

Scanning identifies the available vulnerabilities on your network for cyberattackers to exploit. "A scan will give you the devices connected to that computer and the resources that are operating on that computer, including the specific versions of software applications or an operating system. The device could be a printer; it could be a computer; it could be a blood system analyzer." said Simon.

Protecting against invaders

Simon likens traditional network protection to M&Ms — hard on the outside, soft on the inside. This security approach makes it very hard for malicious traffic to enter the network with strong perimeter defenses, while protections on the inside are more limited. But once malware enters and bypasses that exterior protection, it is easier for it to move around inside the network and obtain credentials for confidential information.

External defenses involve elements like firewalls (solutions that monitor and control incoming and outgoing network traffic), virus protection (software that looks for specific computer code signatures), multifactor identification (similar to the verification code banks send to customers' phones when they log into the system online), data encryption and staff security training.

Employee awareness and staff training are the main protections against phishing, said Scaggiante. "It's not just the technical tools that you put in place and how sophisticated they are, it's also the people in the organization and how you keep them informed and alert about security." The combination of technology and staff awareness and education are the first line of defense.

Another element of defense to address is "bring your own device to work" flexibility that allows staff to connect a multitude of outside devices to a network: smart cell phones, iPads and laptops that have

connected to other networks. These devices are vulnerable to malicious software because they connect to several different networks, not all of which are safe. Think about all the people you see connected to a coffee shop's Wi-Fi. Then these devices are brought to work, increasing the probability that malicious software is going to get into your network.

Protecting bad actors from getting into the system is not enough though. "The second front … is looking at internal activity," Scaggiante added. "I think that every person supporting information security efforts should assume that at some point, somebody who's not supposed to be there will get inside."

Malware counts on minimal or no internal security protections. This lack of internal protection is what makes lateral movement possible. It allows criminals to find a computer and the credentials of someone who has access to the resources that they are seeking. Ultimately, they can find someone who has master access to the whole network.

Simon agreed. "You need the back-end protection … [companies] don't realize that they could stop 99.9% of people clicking on malicious links, but as long as one person in the organization does it, that's all it takes."

When a bad actor does get into the network, organizations need have a plan in place to detect it quickly and stop malicious software from propagating and reaching sensitive data. Information technology staff at the New York Blood Center are using various tools to monitor and assess internal activity. These tools monitor not only information like proper user identification and passwords, but other clues as well. For example, a user could access an internal system with confidential information using the correct ID and password, but they're logging in from China. Intelligent tools can pick up suspicious conditions — login from China is not expected — and

CYBER PRIMER

Malware: Software that is specifically designed to disrupt, damage or gain unauthorized access to a computer system.

Ransomware: Malware that requires the victim to pay a ransom to access encrypted files. (This is what happened to the NHS in 2017)

Phishing: Attempts to gain usernames, passwords and other sensitive information by pretending to be a trusted individual. Phishing emails are the classic example. A criminal is able to send an email that appears to come from someone in the organization or another trusted individual. Relying on this trust, the criminal may gain usernames and passwords, other confidential information OR may download malware when the recipient clicks a link in the email.

Drive-by: An automatic download of malware from an infected website.

Copycat: (1) Using someone else's personal information to pretend to be them for financial or other gain. (2) Using the same or very similar hacking signature.

Virus: Computer code that, like a biologic virus, copies itself once in the network and is harmful to the system — corrupting the system or destroying data for example.

Malicious Hacker: Someone with computer expertise, who uses their skills to circumvent network security, in order to steal and exploit or sell data, or to vandalize.

Inside Attack: An authorized individual infects networks with malware.

Lateral Movement: Using connections between computers, devices and systems to access more valuable and secure data.

Scanning: Identifying connections between computers, devices and systems to move laterally,

alert IT staff. "This is a completely different way of protecting the company," said Scaggiante. "Now you have to basically look inside your organization at the activities that are happening and determine if there is anything that you need to worry about."

Doing more with less

Of course, layers of protection and sophisticated tools require investments and resources, which are tight in even the largest blood systems today. Blood banks do not have the same level of resources as for-profit organizations do. At the same time, the information they work with is very valuable. There are no easy answers.

"You need to be selective," Scaggiante said. "You need to be clever in how you make investments." At the New York Blood Center, IT staff are taking a risk-based approach to identify the weak points and the highest risks. "We address those high risks first."

Technology, like firewalls and antivirus software, can identify suspicious activity but it is crucial for IT staff to follow up on alerts. Dedicated IT personnel are essential to prioritize vulnerabilities and devise solutions. "One of the main challenges that I observe when I am discussing with other blood centers this topic, is that not every blood center has the luxury of an information security expert. In terms of resources, the most important investment that a blood center can make is to have ideally a person who is dedicated [to information security]," said Scaggiante. "If not, at least have a person in the IT group who really understands information security and can dedicate a good portion of their time just focusing on what is the risk, where is our information, how do we protect it, how do we monitor it and how do we respond to threats."

What are we talking about in real monetary terms for bare minimum cyber protection and resiliency after an attack? According to Simon, "I would say that any organization that has an IT budget in excess of $10,000 a year should be able to allocate at least 25% of that budget for cybersecurity. Because otherwise they're risking the integrity of their business." ■

ENDNOTES

1. Alex Matthews-King. "NHS hack just a 'taste of devastation' of major cyberattack with full cost still unknown, warn MPs." The Independent. April 17, 2018. https://www.independent.co.uk/news/health/nhs-cyber-attack-wannacry-russia-hacking-bot-net-security-warning-a8308701.html. Accessed September 20, 2018.
2. National Audit Office. Investigation: WannaCry cyber attack and the NHS. October 24, 2017. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf. Accessed September 20, 2018.