A Primer on Cybersecurity for Physicians

Uma Introdução à Cibersegurança para Médicos

Nathan C. LEA✉[1], Filip DE MEYER[2]
Acta Med Port 2019 Sep;32(9):563–564 ▪ https://doi.org/10.20344/amp.12542

Keywords: Computer Security; Confidentiality; Physicians
Palavras-chave: Confidencialidade; Médicos; Segurança Computacional

INTRODUCTION

In 2017 a major cyber security risk became a reality. The WannaCry attack crippled the information technology (IT) infrastructure across industries all over the world, including financial, legal and utilities. But the health sector was also hit, most notably the National Health Service across the United Kingdom.

Reports of the impact were stark: cancelled operations, appointments, x-rays, delays in dispensing prescriptions and to chemotherapy appointments. A report by the Chief Information Officer for Health and Social Care detailing the impacts and response is available.[1]

Data security had featured in a major review by the National Data Guardian and Care Quality Commission a year before the WannaCry incident.[2] The review called for better communication, sharing of expertise and good practice, and real commitment to updating IT infrastructure and development of basic standards to achieve this expediently. But two years on, it is worth pausing and asking: has the health sector internationally learned the lessons of WannaCry?

The need for awareness

Fortunately, all industries that rely on data had to take notice of risks around data, its security and protection. In an editorial last year, we looked at it as an opportunity for culture change and highlighted the implications of WannaCry.[3] GDPR requires anyone handling personal data to do so securely. Whilst an essential principle, it is not very specific on what that entails, but the health care sector is listening and cannot afford to ignore this after what we have seen in 2017.

There is a clear need for everyone using and relying on cyber systems and services to appreciate the basics as well as deferring to specialist expertise in cyber security and risk management to help make things safer. This is part of a process that ensures you and your health organisations can prepare for ensuring that your systems can operate, and you can adapt to evolving risks whilst enjoying the benefits that a more digitally driven health service can reap.

We hope the following summary will help get readers thinking about how they can work more securely and advocate for cyber security to become a standing item as business as usual so that nobody has to cope with the delay to the anxiously awaited surgery or treatment because a virus crippled an IT infrastructure, the software was not patched, there was no antivirus and / or the firewall was not configured.

The points below are intended to help you think about security and cyber safety more generally. You should consider this as a basic introduction, but it is no way exhaustive. Our aim for this is to provide general guidance, from where you will be able to seek more advice and incorporate this area more into your day to day working practice. The European Union Agency for Network and Information Security (ENISA)[4] is a good general resource for information.

1. Keep software up to date

Where you have a managed infrastructure, ensure the people who are managing it have the resources and expertise to maintain up to date software. We often can find that a beloved Electronic Healthcare Records system that has been running for years can only continue to run on software that is no longer supported by the vendor (e.g. Windows XP). Updating the existing systems will require investment so make sure that is recognised and you have the resources available to do it.

If you rely on managing your own Information and Communication Technology as a practitioner using laptops and smart phones for example, think carefully about how you achieve this. Software upgrades are inexpensive, and support is at hand. Do not cut corners here — it is worth spending a few hundred extra euros a year to avoid having to explain to your patients and regulators why data was compromised and you had to cancel appointments because you were using software that is no longer patched by the vendor after you had been warned. But think very carefully about whether you need a service to support you or at the least offer a sanity check to ensure you are covering what you need (see item 4).

1. University College London. London. United Kingdom.
2. Department of Public Health and Primary Care. Faculty of Medicine and Health Sciences Ghent University. Ghent. Belgium.
✉ Autor correspondente: Nathan C. Lea. n.lea@ucl.ac.uk
Recebido: 09 de julho de 2019 – Aceite: 09 de julho de 2019

2. Malware and antivirus

It is worth looking at ENISA's top 15 cyber threats page[5] to get a sense of the scope and scale of threats. Antivirus subscriptions are essential and can help defend against many of these — any computer will be subjected to a barrage of emails, remote server communications and even software scams that contain viruses, worms and all the other malware that is in circulation around cyberspace.

There are a host of antivirus companies who can supply a subscription to update and support your virus definitions and actively scan your infrastructure, either managed by a large healthcare provider or by you as a sole practitioner. It is worth looking for a subscription that suits your infrastructure.

Organisations such as Open Web Application Security Project (OWASP)[6] and others keep a set of advisory and guidance around security regularly updated. The security of website development can significantly be enhanced by following the OWASP development guide and by running one of the vulnerability scanning tools, such as recommend by the OWASP community.

3. Infrastructure

Computers and servers are like massive telephone exchanges and you must be able to not only screen the communications that are coming from other machines, but also actively stop them. This is where firewalls and intrusion detection systems are key. Firewalls allow you to control what "ports" computers are allowed to listen on for communications from other computers, where registries of known "dangerous" ports are kept. These ports can be switched off when they are not being used for legitimate, safe communications.

Intrusion detection allows your servers to listen on firewalls for any patterns of communication that are known to be suspicious so that you can take action to prevent the communication and screen out anything potentially harmful. The Center for Internet Security maintains a list of Cybersecurity threats that are worth reviewing.[7]

Apart from the (possibly changing) IP addresses of your systems, various applications and communications protocols are assigned either dedicated port numbers or are borrowed from a pool of non-reserved numbers. All ports should be blocked from incoming and outgoing traffic, except those necessary for the communication protocols in use.

Firewalls regulate the flow of network traffic, blocking obtrusive attempts to find a way into a system but allowing necessary traffic.

4. Seeking and sharing the knowledge

The Care Quality Commission review in 2017 highlighted the importance of sharing knowledge. It recognised that people were at one and the same time the biggest security risk but also the most powerful weapon in the management of cyber risk. In this case, if you are uncertain or worried, ask someone who knows. Within a managed environment you will have digital services teams who are responsible for providing the assurance that you need, and if your health provider does not offer this or at least subcontracts a company, they should think about how to manage the very real cyber risks.

As a practitioner you may want to ensure that you have access to experts and advisory about these areas. Think about your own needs and the time you have available to spend on managing these kinds of technical details. It is commendable if you have the know-how to do this of course, but it never hurts to make sure you are not yourself over stretched as the costs involved in managing this in a secure and accountable way are far lower than the financial and reputational costs if you get it wrong.

In conclusion, cyber security must be as core to healthcare operation and as keenly managed as medications, surgical equipment and hygiene. We looked at these kinds of issues with the advent of GDPR, but for that, and cyber security, we repeatedly see that it is far better to seek clarification on what to do than beg forgiveness when something goes wrong that could have been prevented. Cyber security is not a mystical, convoluted idiosyncrasy that can only be divined by wise and eccentric sages — it is core to everyday practice.

REFERENCES

1. Lessons Learned review of the WannaCry Ransomware Cyber Attack. [accessed 2019 May 15]. Available from: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf.
2. Review of data security, consent and opt-outs. [accessed 2019 May 15]. Available from: https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs.
3. Lea NC. How will the General Data Protection Regulation affect healthcare? Acta Med Port. 2018;31:363-5.
4. European Union Agency for Network and Information Security. Homepage. [accessed 2019 May 15]. Available from: https://www.enisa.europa.eu.
5. ENISA. Threat landscapes. [accessed 2019 May 15]. Available from: https://etl.enisa.europa.eu/#/.
6. OWASP Foundation. Homepage. [accessed 2019 May 15]. Available from: https://www.owasp.org/index.php/Main_Page.
7. Cybersecurity Threats. The CIS® and MS-ISAC® cybersecurity professionals analyze risks and alert members to current online security threats. [accessed 2019 May 15]. Available from: https://www.cisecurity.org/cybersecurity-threats/.