HealthManagement.org
Promoting Management and Leadership

Volume 17 - Issue 4, 2017 - Cover Story: Risk & Danger

Cyber infection control: Time to take it seriously

James Mucklow
******@***paconsulting.com

Digital healthcare expert - PA Consulting Group London, UK

LinkedIn Twitter

Richard Corbridge
Editorial Board Member
HealthManagement
******@***nhs.net

CIO - Health Service Executive (until 2017)
Dublin, Ireland
CEO - eHealth Ireland (until 2017)
Dublin, Ireland
Chief Digital Information Officer - Leeds Teaching Hospital NHS Trust
Leeds, UK

LinkedIn Twitter

Both infection control and cybersecurity support the whole care process, but why do we treat them so differently?

In 1847 the father of infection control, Ignaz Semmelweis, took a position running maternity services in a Vienna hospital. During his time there he observed that women cared for by physicians were more likely to die (13-18%) from infection than women cared for by midwifes (2%). This led him to develop a theory that infection control was critical. He then implemented mandatory handwashing and saw the mortality rate from infection drop to 2%. Since then infection control has been a key part of all aspects of the care process. However, the question why physicians washed their hands less than midwives though was never really answered.

Today, health organisations face a new infection challenge, that of keeping their IT systems free of viruses and other attacks on their health, and they will need to treat this threat with the same seriousness.

IT is crucial to care in the 21st century

This starts by understanding that digital technology is now integral to healthcare. It touches all parts of the process: clinicians look at records electronically, lab tests are computerised, and ambulances are dispatched by computers. This role will continue to increase as we move to paperless, integrated and patient-centred approaches.

The risk of an attack on these systems will increase as they are accessed by and connected to others and the ownership and responsibility for their cleanliness gets blurred. For example with mobile carers, carers using Bring Your Own Devices, and patients wanting to contribute data from a fitness tracker—who is responsible for the digital cleanliness?

On 12 May 2017 the *Wannacry* computer malware provided a dramatic illustration of the risks. A significant number of global care organisations saw their work disrupted, and many more breathed a sigh of relief that they were not affected. While almost 50 services have been affected by malware and IT service failures in previous years, none have ever hit this hard or with such a global reach. *Wannacry* was the equivalent of letting two five-year olds loose in an operating theatre before beginning open heart surgery, and showed us all that our systems, our data access, our way of working does not support digital infection control.

Cybersecurity is infection control

In response, we all need to understand why these cyber issues occur, and what we can do to prevent them. This starts with getting the right governance and recognition at board level. Leaving it to junior members of staff means it won't be getting the right attention until it hits the headlines. Boards now need to scrutinise digital cleanliness in the same way as they treat the latest infection control key performance indicators. Worrying about cyber security must not, however, be used as an excuse to avoid embracing digital technology and the opportunities it provides to transform how care is delivered.

In the same way that a ward has a hygiene owner, digital security needs its own champion. The advent of the Chief Clinical Information Officer and its appearance in the Wachter report (National Advisory Group on Health Information Technology in England 2016), for example, go some way to addressing this. In all this digital cleanliness has to be more than the equivalent of a poster asking you to wash your digital hands properly, but be recognised as a critical priority across the organisation.

You might also like: When a Cybercrime Takes Place - Who's to Blame?

In a connected world, cyber risks are Inevitable

Connectivity in health organisations brings real value to patients. For example to support continuity of care, or support peripatetic carers with mobile devices, a connection to the worldwide web is necessary, but that web is a potential source of digital infection. Connecting to it exposes the organisation to risks, and it needs to understand those risks, manage them, be ready for them and react effectively when they inevitably strike.

To do this healthcare providers need a digital strategy and a cyber security and resilience plan, just as they

have an infection control plan. That strategy should be linked to patient care and recognise that it is not just about investing in technology, but in people and training. PA has found that people and behaviours are a factor in over 80% of high-impact cyber breaches. The kind of behaviour that puts information at risk ranges from the completely accidental (unaware), the careless or negligent, all the way to deliberately malicious. The best way to reduce these risks is through training and communication.

Regularly review your security measures and learn from others

The next step is to recognise that cybersecurity is an arms race. Threats evolve over time and so the work is never done, similarly to the increased resistance we currently face with antibiotics. There is a clear need for regular reviews of the threats and security measures, followed up by action to update systems, and update them when security flaws emerge. One organisation we worked with saw four zero-day attacks (these are cyberattacks exploiting a weakness not seen before) in three weeks. That underlines the clear risk if an organisation only updates its security every three months. While software providers have become pretty effective at issuing security patches, their efforts are pointless if the organisation does not have a process for applying those patches quickly.

The patch that protected against the *Wannacry* attack was available two months before it happened, but clearly many organisations were not aware of this and did not deploy it. This underlines that there needs to be a recognition that a cyber risk is like a dirty thumb print on a theatre-ready scalpel, and needs immediate action; cleanliness can be best achieved by providing a hospital with all the tools to reduce infection rather than each individual bringing their own soap and nail brushes to theatre.

Healthcare can also learn from other industries. Mature digital industries have realised that running data centres is not their core skill. So they have moved their IT to the cloud (offsite external providers) and taken advantage of the massive investments, $30bn in some cases, cloud providers have made to provide more efficient, more secure, higher quality services. It is clear that fighting cyberattacks requires a number of layers of defence including an ability to isolate systems that can't be updated. One organisation we worked with had all its systems connected to a single network and that made it very vulnerable to attack. In the same way that a hospital isolates patients to limit the spread of infection, they should do the same with their digital systems.

Lastly they should remember that cybersecurity requires constant vigilance and systems have to be actively managed. This involves monitoring their status and looking for unusual activity and checking antivirus protection, as well as ways to detect intrusion. These activities will help organisations see that digital technology, when it is properly protected from infection, is an asset that allows them to deliver better care.

Key Points

- IT and cybersecurity need to be regarded as key to the care process
- IT systems need to be connected, which exposes them to risk
- Cyber risks need to be managed

James Mucklow leads PA Consulting Group's Digital Healthcare work. He is passionate about delivering better systems to care and new treatments. He has been delivering complex innovative projects for over 25 years across all aspects of the lifecycle. His work primarily focuses on improving patient care and accelerating clinical research. He has been working at PA for over 20 years and prior to that worked at the National Institute for Health Research.

Richard Corbridge is a globally recognised expert in healthcare strategy and technology, with over 20 years' experience in the Health and Clinical Research Information sectors. Richard has a passion for business change and benefits management in health and very much insists on a focus on engagement and benefits being brought to technology implementation.

Published on : Tue, 19 Sep 2017