National Assembly for Wales

Health and Social Care Committee

Access to medical technologies in Wales

Evidence from Westgate Cyber Security Ltd – MT 24

Westgate Cyber Security Limited

National Assembly for Wales

Health and Social Care Committee – Medical Technology inquiry

Effective Friday 18 October 2013

Prepared By:
David Jones, Director

Contact information:

David Jones
Director, Westgate Cyber Security Limited
djones@westgatecyber.com

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

1.1 Background

The National Assembly Health and Social Care Committee is planning to conduct an inquiry into the appraisal of, and access to, medical technology.

Westgate Cyber Security Limited (Westgate) is a specialist Management Consultancy working in the area of information security.

1.2 Overview and Summary

Westgate is presenting the Committee some initial views on the subject of information security in relation to both existing and future medical technology.

Westgate's views can be summarized into the following three points

- *The pace of emerging technology in this domain is already significant, but will grow significantly in coming years, it already includes*
    - *Surgical robots*
    - *Tele-medicine devices*
    - *Portable information-gathering appliances (including consumer smart-phones)*
    - *Information systems*
    - *Data analytics, including the use of publicly available and pseudo-publicly available data (ranging from formal research data such GWASS studies to social media data-harvesting from sources such as Facebook)*

- The Information Governance issues will be increasingly important. Transparency of how the public perceive the use of the data presents a risk to up-take. Appropriate use of data, especially data-sharing protocols are critical. This issue is referred to as **Information Governance** below.

- There is a real and emerging threat from external factors. Conventionally referred to as "hacking", this threat requires a close understanding of the vulnerabilities of both physical devices and information systems. This issue is referred to as **Emerging Risks and Threats** below.

1.3 Limitation of response

This document only seeks to comment on the scope of the enquiry, not set out detailed evidence. Therefore the response is limited to raising and listing some of the key points only.

Furthermore, Westgate's response is limited to the area of Information Security only.

It does not include the following:

- Decision-making processes in NHS Wales

- Funding for technology
- Accessibility
- Appraisal of technology

2 INFORMATION GOVERNANCE

1. There are a number of Welsh Government systems, protocols and processes in place surrounding the governance of information.

   These include, but are not limited to
   a. Data-sharing protocols (WASPI)
   b. Formal Information Governance roles (the Caldicot Guardian, usually held by the Health Board's Medical Directors)

2. The issues of transparency are key. The public need to both understand and respect the processes surrounding the data.

3. "Ownership" of medical information is an issue that is not sufficiently clear. Patients are service-users are right to think that the data on their health (effectively, their Medical Record) is owned by them, but the usual conventions of ownership are not in place.

3 EMERGING RISKS AND THREATS

Some of the most interesting developments currently taking places are in the area of physical Medical devices and tools. These range in complexity from small tele-medicine devices to fully functional surgical robots, capably of undertaking orthopeadic operations.

The threats and risks fall into two areas:

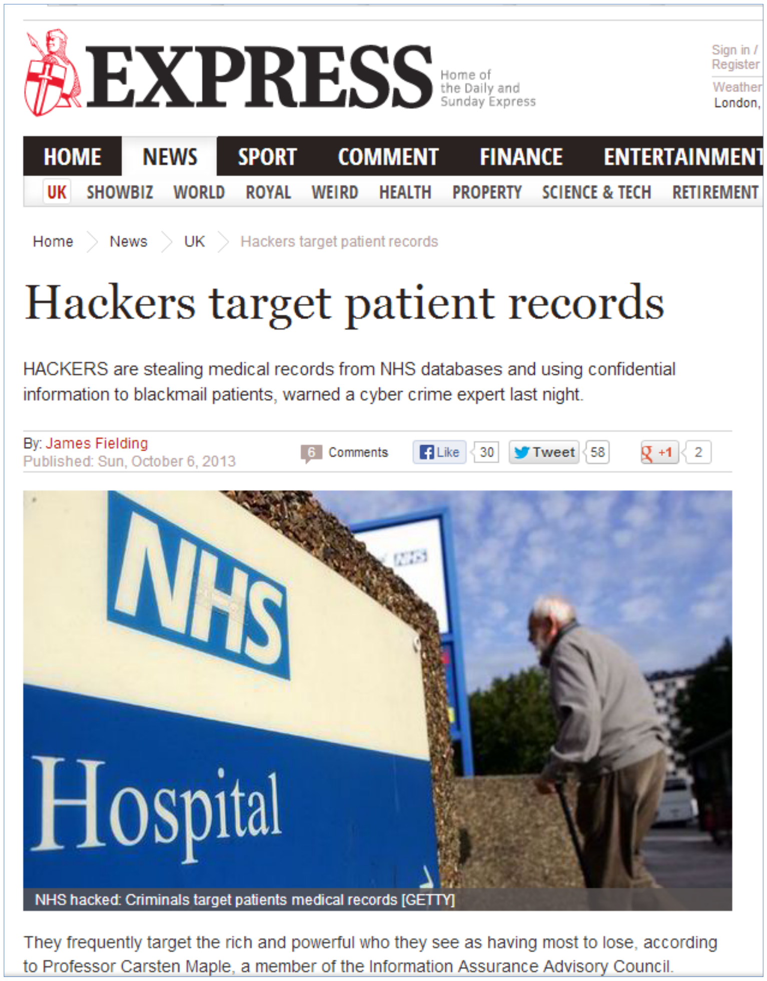
a. Internal Factors.

The failure of any kind of device poses clear problems of reliability and also reputational loss. Often these failures of hardware, software or communication technology are quality issues, which can be mitigated by quality assurance processes.

Increasingly, the full range of Medical Devices have very sophisticated computers embedded in them. These computers are subject to failure just like any other desktop or Laptop computer, but they are rarely subject to the same degree of scrutiny and testing.

b. External Factors

It is often difficult to imagine why any individual or organization would choose to interfere with a medical device.
Clearly any act of this kind is both wrong and dangerous, but it is still sometimes difficult to see what motives such an attack.
Unfortunately, that question of motive rarely applies in Cyber Security. A recent news article in the Daily Express revealed how attackers are stealing patient records with a motivation of blackmail and extortion. Whilst this does not directly apply to Medical Devices, it reveals the complex nature of motivation.



Hackers target patient records

HACKERS are stealing medical records from NHS databases and using confidential information to blackmail patients, warned a cyber crime expert last night.

By: James Fielding
Published: Sun, October 6, 2013

NHS hacked: Criminals target patients medical records [GETTY]

They frequently target the rich and powerful who they see as having most to lose, according to Professor Carsten Maple, a member of the Information Assurance Advisory Council.

This is a real and growing treat.

Within industries such as energy and transportation (collectively known as Critical National Infrastructure – CNI) there is already a high level of maturity around the issue of the risk from parties intent on external attack. Often this is referred to as Cyber-Terrorism.

England's response

The NHS in England have a body called The Health and Social Care Information Centre (broadly comparable to Wales' NWIS). In July 2013 they began a review of the Information Security Practice, having described the number of attempts to hack the NHS as "considerable".

Whilst this piece of work is not specifically realted to Medical Technologies and Devices, it is clearly related.

4 CONLUSION

Westgate hope that this review includes the issues surrounding information security and information governance.

Our view is that the security of Medical Technology will become an increasingly important issue in the years ahead.

Westgate will be pleased to verbal evidence to the Committee.