5th International Congress of Breast Disease Centers 2015

“MULTIDISCIPLINARITY IN THE BREAST CENTER”

ANTWERP, ANVERS - February 5 - 7, 2015

Edmond Cissé Ph.D.
Senior Security Consultant Manager

URÆUS CONSULT
Nice Sophia Antipolis FRANCE

IBDC 5th International Congress of Breast Disease Centers 2015

uræus CONSULT

Cybersecurity and Identification of content quality

Healthcare IT State Of The Art

- ☞ Electronic health records hosted remotely
- ☞ Telemedicine
- ☞ Robotic surgery

Internet of Things (IoT)

- ☞ Connected medical devices
- ☞ Remote controlled medical devices
- ☞ 26 billion units installed in 2020
- ☞ Healthcare is of the leading adopters in 2020
- ☞ Personal devices - BYOD (Bring-Your-Own-Device)

Cybersecurity and identification of content quality

***Cyberattack** is intentional exploitation of computer systems, IT-dependent devices and networks using malicious code in order to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.*

Health care institutions are targeted by hacktivists…

☞ 94% of medical entities assume having been a victim of cyberattacks

☞ 600% increase in attacks on hospitals over the past 10 months

☞ 205 hospitals operated by CHS compromised by a cyber-attack

☞ Theft of security social numbers and personal data of 4.5M patients

☞ Theft of more than $1M from Washington hospital payroll accounts

Medical devices and systems vulnerabilities are actively exploited…

☞ 72% of malicious content or virus directed against healthcare providers

☞ Boston's hospitals attacked every 7s and 98% incoming mails blocked

Cybersecurity and identification of content quality

Risk associated with cyber-intrusion

☞ High financial risk : approx. $233 per-record in case of data loss

☞ Patient health and safety at risk through connected medical devices

☞ Disruption of critical medical infrastructure, services or communication

☞ Inefficient management of patient due to low quality of content

Cybersecurity threats mitigation tools

***Cybersecurity** risk mitigation to ensure the integrity, availability, confidentiality, authenticity and traceability of personal health information.*

☞ Regulations for security and privacy protection (such as HIPAA)

☞ Real-time traffic surveillance and on-the-fly content quality decryption

☞ ISO-27000 family helps organizations keep information assets secure

Cybersecurity and identification of content quality

Conclusion

☞ Cybersecurity must be of greater concern for health care providers

☞ Compliance doesn’t guaranty that adequate security level is reached

☞ Cybersecurity management and identification of content quality are tied

☞ Medical device-makers should enforce their products cybersecurity

☞ Strategies used by public heath to tackle epidemics is applicable

Bibliography

1- Filkins B. SANS health care cyberthreat report : Widespread compromises detected,compliance nightmare on horizon. Norse.February 2014.

2- Perakslis E. Cybersecurity in Health Care, NEJM july 31, 2014, Massachusetts Medical Society, 2014

3 - Orcutt M. 2015 Could Be the Year of the Hospital Hack. Dec 2014, MIT Technology Review (http://www.technologyreview.com/news/533631/2015-could-be-the-year-of-the-hospital-hack/)

4- Lettre d’information Secteur Médical - Santé Cybersécurité des Dispositifs médicaux : un enjeu majeur pour les acteurs de la santé et les patients, Nov 2014 LNE (http://www.vertical-mail.com/sololne1411med/20.php4)

5- Stamford, Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020 Dec, 2013 , Gartner (http://www.gartner.com/newsroom/id/2636073)

Edmond Cissé
edcisse@uraeus-consult.com

uræus
CONSULT

www.uraeus-consult.com