NETWORK SECURITY INFRASTRUCTURE AUDITING FOR MEDICAL SUPPLIERS AND DEVICES

Nimmo Dragomelo
(Quality World)

16 Sectors of Critical Infrastructure Cybersecurity (as practiced USA/EU/UK/JAPAN)

1.0Energy Services Sector/ 2.0 Dams Sector

3.0 Financial Services Sector/ 4.0Nuclear Reactors, 5.0Materials, and Waste Sector/6.0Food and Agriculture Sector/7.0Water and Wastewater Systems Sector

8.0Healthcare and Public Health Sector(Medical Devices)9.0Emergency Services Sector/10.0Transportation Systems Sector/11.0Chemical Sector/12.0Communications Sector/13.0Information Technology Sector/14.0Defense Industrial Base Sector/15Critical Manufacturing Sector Government Facilities/16 Commercial Facilities Sector

NETWORK AND INFORMATION SYSTEM (NIS)(EU DIRECTIVE)

- EU DIRECTIVE FOR NETWORK AND INFORMATION

SYSTEM (NIS) (July 6, 2016)TO ENABLE COUNTRIES TO BE READY TO PREVENT AND RESPOND TO CYBER SECURITY ATTACK.

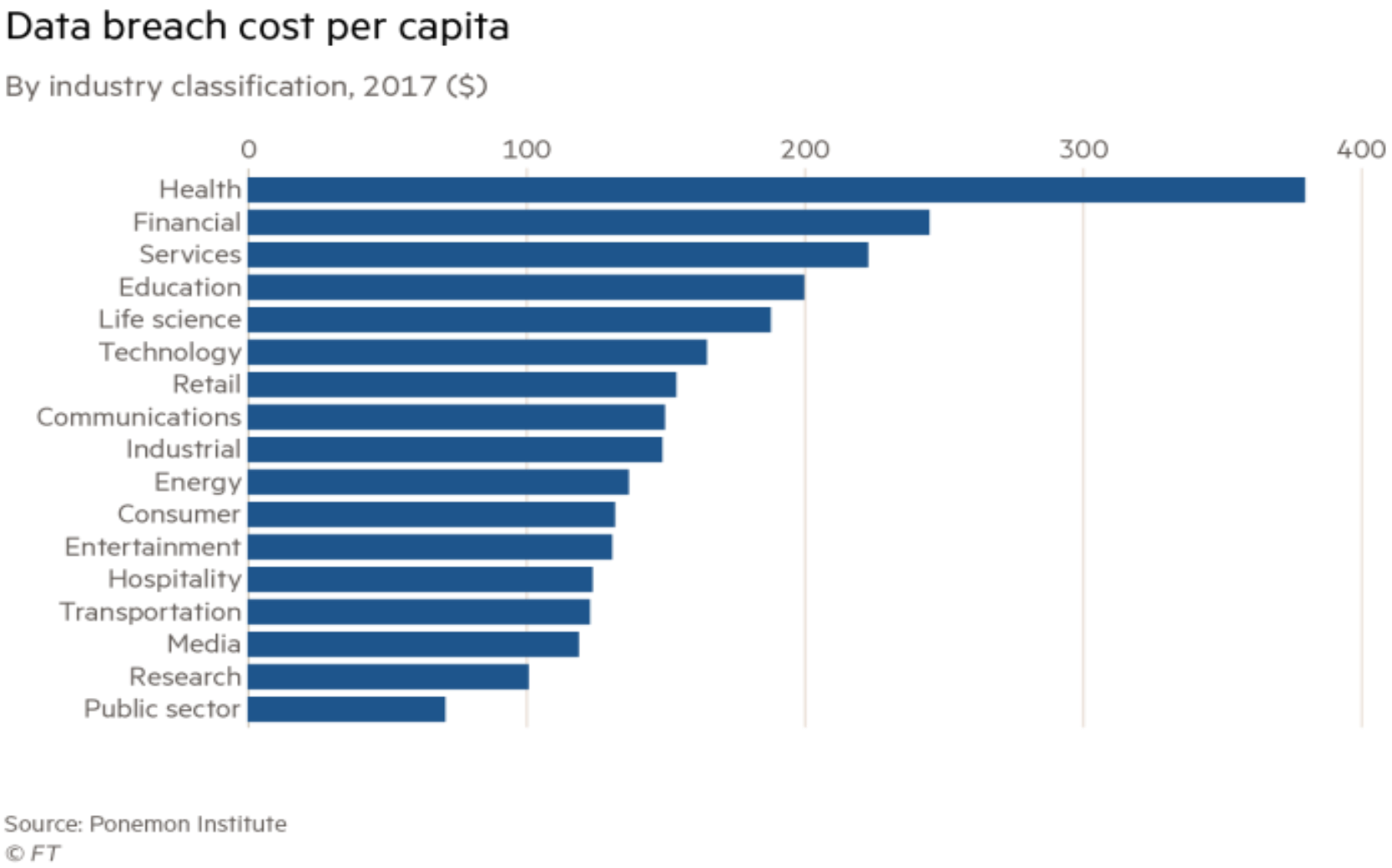
- IT REQUIRES CRITICAL INFRASTRUCTURE

ORGANISATIONS TO IMPLEMENT STRONGER SECURITY ANF BREACH REPORTING FOR ICS/SCADA/OT NETWORKS.

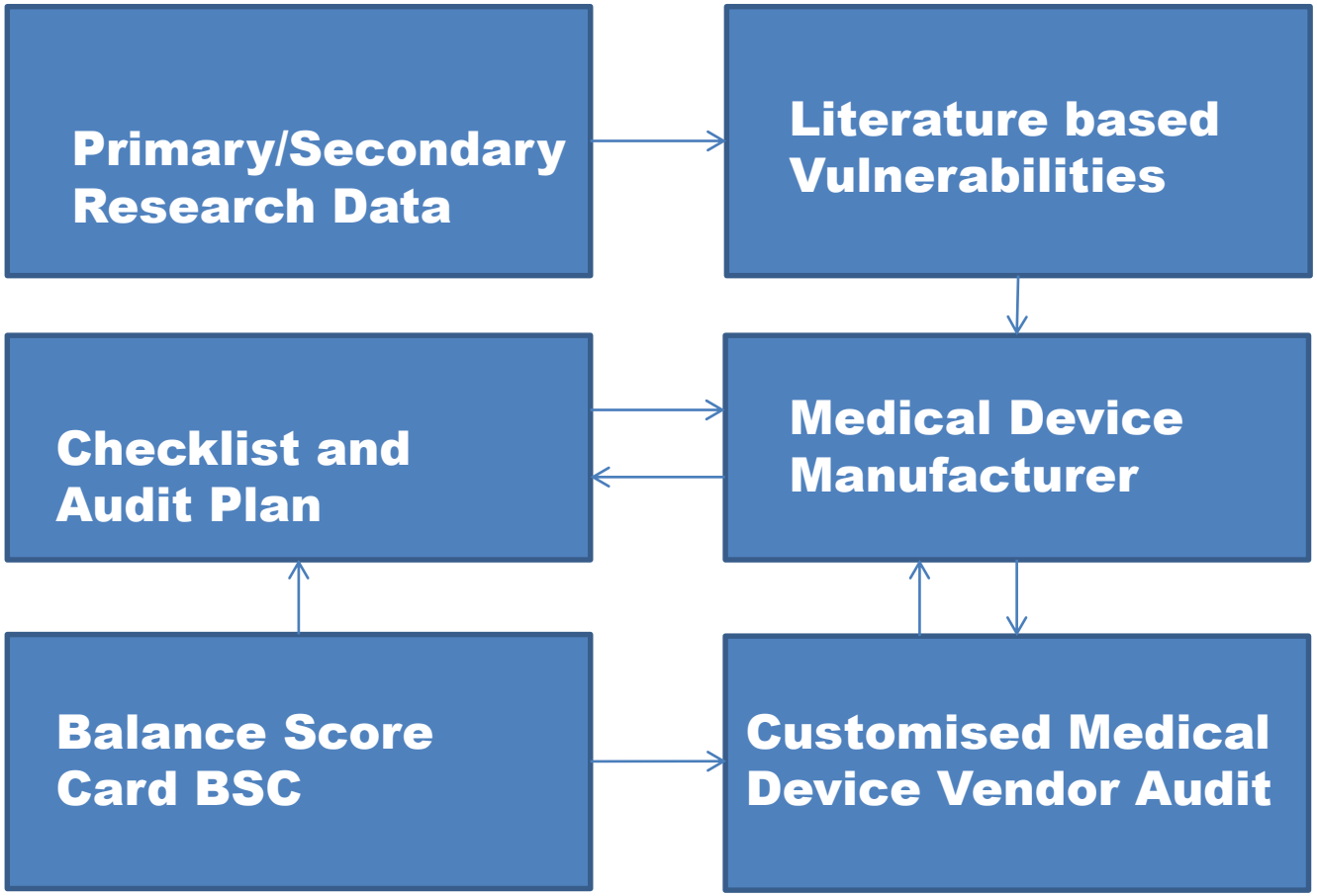
Top 5 Vulnerabilities(NIS)(Medical Devices)(Audit Plan Consideration)

- Limited spending (budget) in Cyber Security
- High Demands of Medical Records in Black Market
- Ransomwire
- BOYD(Bring Your Own Device Policy) Policy
- Employee Negligence

Data breach cost per capita(industry classification)



Methodology Applied(Medical Devices and Suppliers)(as applied in conducting audits)



Key Cyber Security Principles—Critical Infrastructure Health Services –Related to Medical Devices and Suppliers

- Shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices
- Address cybersecurity during the design and development of the medical device
- Establish design inputs for device related to cybersecurity,
- Establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g)

The device is only as secure as it's weakest link"(Source: SDMD)

It is important that healthcare organizations do their part in cybersecurity risk. Responsibility cannot all be held by the manufacturer. The hospital or healthcare providers must ensure that medical device is deployed to an equally secure network system.The subject heading theme is an important consideration in the formulation of an effective Cyber Security audit plan for medical devices and suppliers.

Key Reference Standards(Cyber Security Audits Related to Medical Devices and Suppliers)(Audit Criteria Basis)

- ISO/IEC 27032:2012 Information technology – Security techniques –
- IEC 62304:2006 – Medical device software –This standard is currently under revision and harmonization with ISO 82304.
- IEC/ISO CD 82304 Health software – Part 1: General requirements for product safety ISO/IEC 80001 series of standards detail guidance for Application of risk management for IT-networks incorporating medical devices.
- ISO/DTR 80002–2 Medical device software – Part 2:
- IEC/TR 80002–3:2014 Medical device software – Part 3: Process reference model of medical device software life cycle processes (IEC 62304).
- ISO 13485-2016 Medical Devices Quality Management Systems/Requirements for regulatory purposes
- NETWORK AND INFORMATION SYSTEM (NIS)
- ISO 27001. ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS).

These standards, while providing good practice in risk and development lifecycle processes, do not deal with the fundamental cybersecurity protection required in the environment of use for medical devices as such. An audit plan should therefore be effectively established.

Summary & Conclusion

- In the health care setting, patient safety will always come before cybersecurity requirements. The challenge is to close the gap between the two objectives, minimizing compromise and ensuring patient safety, while being responsive to the evolving cybersecurity threat environment. An effective audit plan with effective audit criteria is therefore the key to addressing medical device related cyber security vulnerabilities. (See research Methodology slide)
- Cybersecurity vulnerabilities that are associated with medical devices are similar to any other networked system. However establishing potential detrimental impact on patient safety that exploitation of cybersecurity vulnerabilities may have is the primary aim of the security audit, NIST Cybersecurity Framework is considered an essential IS audit/assurance program criterion that provides management with an assessment of the effectiveness of cybersecurity processes and activities including identify, protect, detect, respond and recover.