TÜVRheinland®
Precisely Right.

AN INTRODUCTION TO MEDICAL DEVICE CYBER SECURITY
A European Perspective

Nigel Stanley
Practice Director – Cyber Security
OpenSky UK, a TÜV Rheinland Company

Mark Coderre
National Practice Director/CISO
OpenSky US, a TÜV Rheinland Company

October 2016

TÜVRheinland®
Precisely Right.

Contents

Executive summary 2
Introduction 3
What is cyber security? 3
The basics 4
Vulnerabilities, threats, impact and risk 5
Medical device risk 5
Medical device hacking in practice 6
Defending medical devices - system testing 7
Defending medical devices - corporate and end user cyber security 8
Medical device compliance and regulatory requirements 9
Introduction to key EU medical data protection requirements 9
European Data Protection Directive (Directive 95/46/EC) 9
Personal data 10
General Data Protection Regulation 11
US-EU Safe Harbor program and Privacy Shield 11
Privacy Shield 12
Key medical device cyber security related guidance, standards and requirements 13
Next actions 14
In summary 15
About the authors 16
About TÜV Rheinland and OpenSky 17
References 19

Executive summary

As in many other walks of life cyber security risks are challenging the medical device manufacturing community on a daily basis. As hackers look for ever more esoteric and challenging targets it was inevitable that medical devices would start to become an attractive area for research and potentially criminal activity.

Regulators and legislators are acting as fast as they can to ensure that data protection laws and device testing standards reflect this new risk, but inevitably they fall behind the hackers in a fast moving race. As devices contain ever more complex software and developers rush to get new features completed the need to write secure code often comes a poor second, potentially exposing devices to attacks that can be conducted locally or even from outside a clinical setting.

For device manufacturers wishing to launch products in Europe recent changes to data protection requirements have forced many to have a rapid rethink in how they process personal data and challenging the previously held notions of patient consent.

The good news is that with the assistance of experts in cyber security and product testing device manufacturers can get ahead of the curve and build vibrant, secure, international businesses that embrace modern, internet based technologies.

Introduction

The past few years has seen huge leaps in the capability of medical devices, fuelled by advances in materials technology, health analytic models, local processing power and the ubiquitous World Wide Web to facilitate device communications.

As medical device technology continues to evolve it is inevitable that more use will be made of commoditised hardware and software. Quite rightly, smartphones are increasingly used as the patient-to-device interface as they provide local processing power alongside an ability to connect into the World Wide Web and transfer fitness (and increasingly clinical) data back to hospitals, family doctors and researchers. In turn these users will wish to analyse and process data on clinical systems and databases, often spread across multiple countries.

This boon to device usability and the patient experience comes with a downside – the ever increasing threat of device compromise, hacking and disruption. Although cyber risk is a consideration in all industries and sectors few could claim to have the direct and possibly fatal consequences that a compromised medical device may have.

It is not only cyber threats that are increasing.

Regulators and legislators are piling on the pressure as they start to force medical device manufacturers to ensure their devices are fit for purpose and at the very least have addressed basic threats and have removed vulnerabilities from device code. Data privacy issues continue to concern users and legislators. Changes to regulations that address data transfers from the EU to the United States continue to force manufacturers into rethinking how they process data to maximise the commercial benefit alongside protecting the patient.

Increasingly medical device manufacturers are now working with trusted third parties' expert in cyber security and conventional device testing to address these risks and smooth their market entry.

What is cyber security?

Cyber security is variously defined, but can be thought of as the protection of information systems, computers and other hardware, and the software and data that runs on these devices.

Few would doubt that the term cyber security has hit the popular headlines. The term cyber means different things to different people, but has certainly entered the public vernacular in relation to computer hacking, data breaches and losses of huge amounts of customer and patient information.

As businesses adopt an ever increasing online presence coupled with social media, e-commerce and smart devices, criminals and bad actors have realised there are richer

pickings online than there ever were in the world of physical crime. Indeed, we have a perfect storm of technology proliferation, intense economic pressures, a changed business environment and a younger generation coming to work with an “always on” mentality. All of these factors combine to create more opportunities for hackers.

But what about the world of healthcare, and in particular medical devices?

As access to the World Wide Web, colloquially referred to as the internet, becomes ubiquitous it was inevitable that medical device manufacturers would harness this capability to make their devices easier to use, manage and maintain. Coupled with the ability to get near enough real time data from such devices, costs have generally been driven down and utility has improved. But cyber risks are increasing.

The basics

Almost every discussion of cyber security relates back to the confidentiality, integrity and availability (CIA) triad.

Understanding cyber security in the context of this triad can help focus thinking and decision making.

- **Confidentiality** prevents sensitive data from being seen or accessed by the wrong people whilst ensuring that those that have legitimate need to access the data can do so. For example, data encryption can encode medical data in a way that only holders of a decryption key can read it. Arguably encryption is the fundamental primitive most used to protect patient data.
- **Integrity** means ensuring that data remains accurate and consistent for its lifecycle. For example, it is vital to ensure the data integrity of medical results, preventing hackers from altering a diagnosis from a positive to a negative or maybe altering blood type or allergy data.
- **Availability** refers to the importance of keeping computer systems online and accessible when required by the business. Denial of service (DoS) attacks are a common hacking technique used to overload computer resources so they are unavailable to legitimate users. Clinical work will soon draw to a halt if supporting computer systems were taken off line in such an attack.

Most medical device cyber risk issues will fall into one of these categories, which make for easier understanding of why a particular technical control or process has been implemented. It is interesting to note that while healthcare networks are extremely focused on confidentiality with medical devices integrity is arguably the most important tenant. When addressing security all issues must be considered but prioritisation must tie back to a risk management process.

Of course other information security properties need to be considered such as non-repudiation (in data security terms the ability to prove data integrity, origin and authenticity), accountability and reliability, but the CIA triad forms the foundation of this work.

Vulnerabilities, threats, impact and risk

When discussing medical device cyber risk, it's important to agree on some definitions and common language:

- **Vulnerabilities** are flaws or weaknesses that expose a system or process to compromise. A good example, familiar to many, is a vulnerability or flaw that is discovered in software and then needs to be patched with updated code.
- **A threat** is any combination of attacker means, motive and/or opportunity and is the potential for a deliberate or accidental exploitation of a vulnerability. Not all threats are deliberate; for example, the accidental loss of a laptop containing unencrypted patient data on a train can have as devastating an impact as a deliberate hack of a medical data web site.
- **Impact** is the negative outcome(s) associated with threats introduced through vulnerabilities to a specific asset or service.
- **Risk** can be defined as the potential of losing something of value, losing the value of something or undesired outcomes. Every medical facility faces risks ranging from a patient tripping over through to the destruction of a hospital during a fire. Executive leadership teams will spend a lot of their working hours evaluating risk against opportunities to grow and develop the facility. Medical device cyber risk is another risk category to be assessed and rated both inherently and residually in device manufacturer's risk registers.

Medical device risk

Medical devices will often contain complex electronics (often electromechanical) with supporting software or firmware. The latter is often used to control specific features of a device and will often be loaded directly onto a chipset. Historically firmware was rarely updatable, but manufacturers are aware now that updateable firmware makes a device easier to support and update against cyber related threats.

There are a large number of potential risks to medical devices, but more common examples include:

- **Flawed or defective software and firmware**. Writing software code that is free of security issues is very difficult. In many instances software developers have not been

trained to write secure software and are unaware of the risks. In many cases the software has not undergone a test to check for security issues.

- **Incorrectly configured network services**. This could include the use of unencrypted connections to the internet resulting in patient data being transmitted in plain/clear text. Attackers could take advantage of open network services and use them as an entry point on a device.
- **Security and privacy issues** such as the use of poor passwords or excessive permissions where a basic user can access administration features. It is not uncommon to see passwords written down and taped or stuck to the device. Passwords may also be "hard coded" in a device, making their retrieval by hackers simple.
- **Poor data protection.** This may occur due to the absence or poor use of data encryption. If used properly encryption is a powerful mechanism to protect data at rest and in transit (i.e. as it is being sent across a network). Most failures in data protection stem from incorrect use of encryption keys and poor technical implementations.
- **Improper disposal or loss of the device** with on-board memory still containing patient data. The secure destruction of the device needs to be factored into the cost of ownership and the disposal process documented and audited. People lose smartphones every day, but if such a device has patient sensitive data on it the medical device manufacturer could be subject to a regulatory investigation.
- **Malware and spyware targeting medical devices**. Hackers and cyber criminals look for the easiest return on their investment of time and money for each attack. Medical devices may not yet be subject to more general cyber-attacks, unless by mistake, but targeted attacks for specific nefarious purposes must never be discounted.

Medical device hacking in practice

In July 2015 there was a hack involving the Hospira Symbiq Infusion System that culminated in an FDA Safety Communication Alert. [1]

Hospira and an independent cyber security researcher identified that the infusion system could be accessed through a hospital's network that could, in turn, allow an unauthorised user to take control of the device and change the dosage delivered by the pump. Neither the FDA or Hospira were aware of such an incident occurring in a healthcare setting but the Symbiq Infusion System was withdrawn from sale, apparently due to unrelated issues. Concerns were raised that although the product had been removed from sale it could still be obtained from third parties. The Department of Homeland Security released a similar advisory [2].

The flaws in the product were reported as including wireless, public and private keys being stored in plain text on the device, a lack of authorisation checking on the devices, and their vulnerability to either a denial of service attack or remote code execution. [3]

In March 2016 ICS-CERT (Industrial Control Systems Computer Emergency Response Team, part of the United States Department of Homeland Security) released an advisory note with regard to vulnerabilities found in a hospital supply system. [4]

Independent researchers, in collaboration with the product vendor CareFusion, identified numerous third-party software vulnerabilities in end-of-life versions of CareFusion's Pyxis SupplyStation system. The Pyxis SupplyStation was obtained through a third-party that resells decommissioned systems from healthcare systems, and the vulnerabilities were found using an automated software analysis tool. CareFusion was provided with compensating measures to help reduce the risk of exploitation for the affected versions of the Pyxis SupplyStation systems.

Defending medical devices - system testing

The technical testing of medical devices is a vital part of the device manufacturing process and helps manufacturers achieve a reasonable level of patient safety. During this process attack vectors, security-critical vulnerabilities and related architectural flaws will normally be discovered and then presented alongside remediation options and a clear understanding of any residual risk.

Typical system testing would include one or more of the following:

- **Threat modelling** to assess attack vectors unique to a product. This will help determine the best applicable security controls.
- **Source code review** this will include a review of software code seeking defects.
  A penetration (pen) test can be undertaken to simulate an external hacking attack that assumes the hacker has no inside knowledge off the device beyond that which they can find out by probing the hardware or using information in the public domain. More usually the pen test will utilise information provided by the manufacturer including full source code and access to supporting documentation. This test may be more thorough and will often uncover more detailed security issues than the first approach. Fuzz testing, where random traffic patterns are sent to a device over time can also be undertaken to ensure resilience to unplanned input. Penetration and software tests should be conducted by device manufacturers on a regular cycle, and certainly if there are changes to the code base that are likely to introduce security flaws.

- **Controls assessment** – review of device security controls against appropriate standards including HIMSS/NEMA Standard HN 1-2013, Manufacturer Disclosure Statement for Medical Device Security (the MDS^2 form)

Defending medical devices - corporate and end user cyber security

Alongside testing of the medical device it is crucial that supporting IT systems are appropriately risk assessed and secured. This applies to the systems used by the medical device manufacturer, the clinical environment and the patient.

The device manufacturer will by necessity use supporting services ranging from email through to file sharing, design and manufacturing software, medical device data systems and network file shares. All of these need to be secured from attackers who will search for the weakest link to conduct their attack. The manufacturer's supply chain will need to be examined to ensure that suppliers adhere to proportionate cyber security control measures as hackers will often look for weakness in a supply chain as an entry point to start an attack.

There must be governance, policies and procedures that are robust and fit for purpose underpinning all corporate cyber security. These elements determine how corporate assets are protected and should reflect the nature of the business and the risk appetite of the leadership team. The commitment of the leadership team is vital in setting the overall corporate tone on cyber security.

Once deployed into the clinical environment device data will often traverse networks out of the device manufacturer's control in places such as hospitals and clinics. Whilst subject to their own challenges and compliance requirements the clinical environment may have limited security resources and certainly their key concern will not be to focus on a specific manufacturer's data security requirements. In practice it is probably better for a device manufacturer to consider the clinical IT environment as being the "Wild West" and apply their own technical controls rather than relying on those that may be in a hospital or clinic. Hospitals should focus on compensating controls for typical medical device residual risks as presented through reporting formats such as MDISS MD-RAP or HIMSS MDS2. Example control areas include asset management, configuration management, clinically appropriate centralised authentication, trust zoning of networks and governance, risk and compliance (GRC) capabilities to aggregate risk from the reports.

For devices that are supplied to patients for use outside of the clinical environment even more consideration needs to be applied to the cyber security challenges a medical device may face. This problem becomes more acute when considering a user may need to connect devices via their smartphones to medical device data services or similar. What measures have been put in place to educate and inform users how to protect their data? What controls have been implemented to manage a lost smartphone that may contain sensitive

medical data? And finally, what measures have been put in place to adhere to legal and regulatory requirements for protecting patient data on its journey from the medical device, through the medical device data service and back to a manufacturer – in many cases in another legal jurisdiction?

Medical device compliance and regulatory requirements

Every organisation is subject to cyber risk related regulations and compliance requirements. These may apply only to specific sectors such as healthcare or financial, or have broader national or even international remits. It is important for every medical device vendor to understand the compliance and regulatory requirements that apply to them and determine how best to manage the various detailed requirements.

Introduction to key EU medical data protection requirements

Medical device manufacturers must understand EU laws underpinning data protection and privacy. This legal framework is subject to change and needs to be monitored on a regular basis but it impacts any device manufacturer that processes personal data.

The European Union (EU) comprises 28 countries that form an economic and political union. The EU single market allows free movement of goods, capital, services and people between every member state.

The EU has two mechanisms to promulgate its legal requirements:

- Directives. These are legal acts of the EU that require every member state to achieve an outcome but the means of achieving that outcome are left to individual states to decide.
- Regulations. These are legal acts of the EU that are self-implementing and do not require the enacting of local, national laws.

For example, Directive 95/46/EC (called the Data Protection Directive) protects individuals with regard to the processing and the free movement of their data. This was enacted in the UK (an EU member) as the UK Data Protection Act 1998.

European Data Protection Directive (Directive 95/46/EC)

Directive 95/46/EC is the base reference text used throughout Europe for the protection of personal data. It sets strict limits of how data can be collected and used and requires each Member State to have a national body responsible for supervising activities concerning the processing of personal data.

Under this Directive data processing is only lawful if

- the data subject has unambiguously given consent; or
- processing is necessary for the performance of a contract to which the data subject is party; or
- processing is necessary for compliance with a legal obligation to which the controller is subject; or
- processing is necessary to protect the vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party; or
- processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

Outside of these requirements the processing of personal data is illegal and action can be taken. It must be noted that 'processing' has a very broad definition within the legislation (e.g. merely reading medical device data from a computer screen displaying personal data is considered to be 'processing' that data.)

Personal data

Much of data protection legislation hinges on the definition of personal data. The UK Information Commissioner defines personal data as follows:

> ***Personal data*** *means data which relate to a living individual who can be identified –*
>
> *(a) from those data, or*
>
> *(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.*

It has been held by the UK Information Commissioner that data that is being processed that identifies individuals by a unique reference number (i.e. patient serial number) and that can be cross referenced with another set of data to identify an individual is personal data. In some geographies or legislations personal data may be referred to as 'personally identifiable data' (PII). For the purposes of this paper these terms are synonymous.

General Data Protection Regulation

The European Data Protection Directive (Directive 95/46/EC) was introduced in 1995. As a directive it was interpreted by member states individually and then written into national law. In January 2012 the European Commission presented a draft proposal to form a new Data Protection Regulation, now called the General Data Protection Regulation (GDPR). The Regulation was adopted in April 2016 and will be applied from May 2018 onwards. As a Regulation it does not need enabling legislation in member states to come into force.

GDPR now includes:

- A single set of rules on data protection that will apply to all EU member states;
- A requirement on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. This must be within 72 hours of the organisation becoming aware of such a breach;
- Requirement for explicit consent for data to be processed. (i.e. opt-in rather than opt-out.) Such consent must be concise, transparent, intelligible and easily accessible. It must be written in clear and plain language;
- The need to appoint a data protection officer if a company carries out large scale monitoring of individuals; and
- Significant fines that are tiered for non-compliance. A maximum fine of EUR 20 million or up to 4% of the annual worldwide turnover in case of an enterprise, whichever is greater.

The new Regulation is expected to focus both companies and individuals on the importance of protecting user data.

US-EU Safe Harbor program and Privacy Shield

In 2000 the US Department of Commerce worked with the EU to create a streamlined mechanism for US companies to meet the requirement of Directive 95/46/EC. This reflected the different approach taken by the EU and the United States for the protection of an individual's privacy and allowed data to be transferred in situations that did not previously meet EU adequacy rules for privacy protection.

A US company could voluntarily decide to join the US-EU Safe Harbor program. Once a participant, the company had to publically declare that they comply with US-EU Safe Harbor requirements and self-certify annually to that effect.

In October 2015 the Safe Harbor program was deemed to be invalid by the European Court of Justice. This followed a legal case that began in 2013 after Edward Snowden released confidential material from the US National Security Agency (NSA). The material provoked concerns about the use of EU data stored by US companies and the possibility that it could

be subject to US government surveillance. The European Court of Justice found that Safe Harbor data privacy provisions were inadequate and invalidated the Safe Harbor agreement with immediate effect.

Privacy Shield

On 2 February 2016 the European Commission and the U.S. Government reached a political agreement on a new framework for transatlantic exchanges of personal data for commercial purposes, called the EU-U.S. Privacy Shield. The Commission finalised the adoption procedure on 12 July 2016.

The EU-US Privacy Shield is based on the following:

- Strong obligations on companies handling data;
- Clear safeguards and transparency obligations on U.S. government access;
- Effective protection of individual rights; and
- An annual joint review mechanism.

The Privacy Shield program, which is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce, enables U.S.-based organisations to join the Privacy Shield Framework. To join an organisation will be required to self-certify to the Department of Commerce and publicly commit to comply with the Framework's requirements.

Alternatives to an organisation adopting the Privacy Shield Framework could include:

- Obtain the full, explicit, unambiguous, voluntary and informed consent of a user for the transfer of their data out of the EU. Applying this retrospectively could be problematic and in practice some member states still maintain that such consent is still inadequate to protect such data transfers;
- Remove all personally identifiable (PII) data and/or encrypt the data so that no PII is contained in the data being transferred. Note that as discussed previously any form of patient reference number or similar that can ultimately be resolved to a patient's actual data (i.e. cross referenced to a patient database, no matter how abstracted the process) will be deemed PII; or
- Setup and maintain a hosted service in the EU so that data is not transferred to the United States.

Key medical device cyber security related guidance, standards and requirements

There are a range of product standards and compliance requirements for medical device manufacturers. New proposals are emerging as legislators gain an understanding of cyber risks (for example the EU's Digital Agenda and Directive on Network and Information Security [5]) and it can be expected that the requirement from regulators will be for more stringent cyber security controls for medical devices in the coming years, not less.

The following represent key regulatory requirements and guidance that may impact a medical device manufacturer wishing to operate in Europe:

- EN 62304:2006. This is the standard for software life cycle processes and creates a framework for activities, processes and tasks. Together these help provide a safe design and maintenance standard for the software. Included in this are proportionate documentation and testing requirements based on the criticality of the software. Criticality is classed A (no injury possible), B (no serious injury possible) and C (serious injury or death possible). Individual software components can attract their own safety individual classification.
- Food and Drug Administration (FDA) Content of Premarket Submissions for Management of Cyber Security in Medical Devices (dated October 2, 2014). [6] This is guidance that identifies cyber security issues for manufacturers and how they should be considered in a premarket submission. Specifically, the guideline recommends that manufacturers define and document the following areas:

    - Identification of assets, threats, and vulnerabilities.
    - Impact assessment of the threats and vulnerabilities on device functionality.
    - Assessment of the likelihood of a threat and of a vulnerability being exploited.
    - Determination of risk levels and suitable mitigation strategies.
    - Residual risk assessment and risk acceptance criteria.

- CLSI AUTO11-A IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard.
- IEC TR 80001-2-2 Edition 1.0 2012-07 Application of risk management for IT Networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls.
- AAMI ANSI IECTIR 80001-2-2:2012 Application of risk management for IT Networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls.
- IEC/TS 62443-1-1 Edition 1.0 2009-07 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models.

- IEC 62443-2-1 Edition 1.0 2010-11 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program.
- IEC/TR 62443-3-1 Edition 1.0 2009-07 Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems.
- IEC ISO 29147 First edition 2014-02-15 Information technology - Security techniques - Vulnerability disclosure.
- IEC ISO 30111 First edition 2013-11-01 Information technology - Security techniques - Vulnerability handling processes.
- HIMSS/NEMA Standard HN 1-2013, Manufacturer Disclosure Statement for Medical Device Security

Next actions

Device manufacturers can embrace cyber related risks by ensuring the:

1. Design cyber security into the product, and ensure that data integrity is considered a top priority alongside its safe clinical use.
2. Undertake a review of the device risks, threats and vulnerabilities and document the findings. Review these findings on a regular basis in light of new and emerging threats.
3. Educate engineers and developers on the importance of data protection and cyber security and ensure that software engineers are recognised for building secure, robust code.
4. Ensure that the device can be safely updated with new software patches and consider how this can be achieved in the clinical environment.
5. Ensure that device software is thoroughly tested and examined, preferably by an independent and objective third party that can apply industry best testing practices
6. Review the data lifecycle so that it is fully understood what data is created and where and how it will be processed through the system. Consider how PII data may be processed and where that data will transit or reside, especially across different legal jurisdictions.
7. Review and keep up to date on the changes to medical devices regulations and laws across the international domain.
8. Create and maintain a risk register. Ensure that any supporting corporate IT infrastructure has been reviewed for cyber related risks and that proportionate controls have been implemented to manage such risks.

9. Implement robust incident response plans so that if a data breach or similar incident occurs it can be dealt with effectively. These should be aligned with existing and anticipated processes from organisations such as MDISS, FDA and NH-ISAC.
10. Ensure that any device installer is fully aware of related cyber security risks and what controls should be implemented to manage or reduce them in a proportionate manner.

In summary

Clearly medical device cyber security risks can be significant and are attracting the attention of regulators and lawmakers. The complexities of cyber security risks grow each day, and as such regulators are not going to reduce the requirement for affected manufacturers to ensure their devices are safe and secure.

The good news is that it is possible to take a proportionate approach to these risks and manage them in a cost effective way by engaging a testing and certification partner with complimentary expertise and a passion to address new and emerging cyber security risks.

About the authors

Nigel Stanley is a specialist in information (cyber) security and business risk with over 25 years' experience in the IT industry. He is a well-recognised thought leader and subject matter expert capable of delivering complex cyber security projects across small, medium and large scale enterprises.

Nigel has in-depth knowledge of cyber security, information security, business risk, data breach incident response, digital forensics, business continuity, cyber warfare, cyber terrorism, mobile device security, BYOD, smartphone security, application development, software development, systems engineering, SCADA and industrial control systems.

He has written three books on database and development technologies and is a regular conference speaker. He is able to passionately bring his technical knowledge together with his practical experience of cyber security and business to help clients derive benefit from information security.

Nigel is a Chartered Engineer and member of the Institution of Engineering and Technology (where he sits on the IET Cyber Security Steering Group), Institute of Electrical and Electronic Engineers and the British Computer Society. He has an MSc in Information Security from Royal Holloway, University of London where he was awarded the Royal Holloway University Smart Card Centre Crisp Telecom prize for his MSc research dissertation.

Mark Coderre is an Information Security Executive with over 25 years of experience protecting information in Healthcare and Insurance. He is now a National Practice Director with OpenSky Corporation focused on CISO Advisory services, Internet Identity, Healthcare, GRC and Risk Management. During his career with Aetna in Hartford, Connecticut Mark served as Executive Director of Security Strategy and Risk Management.

Mark's seasoned approach to information security is leading edge yet pragmatic given his background in both security engineering and security architecture. Mark recently directed the fusion of best practices from the financial sector into healthcare security leading to a world class program.

Mark's leadership earned industry recognition including the 2013 CSO Magazine Award for International Governance, Risk & Compliance, the 2014 RSA/Archer Operational Risk Management Award, and the Liberty Alliance Federated Identity Deployment of the Year award.

About TÜV Rheinland and OpenSky

TÜV Rheinland is a global leader in independent inspection services, founded more than 140 years ago. The group maintains a worldwide presence with 19,600 employees; annual turnover is nearly EUR 1.9 billion. For more than 15 years, TÜV Rheinland has been supporting the private and public sector with comprehensive consulting and solution expertise in IT, cyber security and telecommunications through digital transformation processes.

With more than 600 specialists around the world, TÜV Rheinland provides strategic consulting, design and process optimization through to implementation, operation, or certification of systems. A high level of technological expertise, comprehensive experience in key industries and strategic partnerships with market leaders enable them to create innovative and future-proof ICT solutions.

OpenSky Corporation is part of the TUV Rheinland group and a 100% subsidiary of TÜV Rheinland. OpenSky provides information technology expertise to help corporations optimize IT platforms, protect information assets, and accelerate the adoption of strategic technologies. It specializes in transformational IT infrastructure, security, and risk consulting.

OpenSky's key differentiators include vendor independence, deep industry and technology expertise, and a holistic approach to evolving IT infrastructure platforms.

OpenSky Corporation provides information technology expertise to help corporations optimize IT platforms, protect information assets and accelerate the adoption of strategic technologies. We specialize in transformational IT infrastructure, security and compliance consulting.

We help enterprises with:

- Managing cybersecurity risks
- Planning for IT optimization initiatives.
- Shifting computing to virtual and cloud based infrastructures.
- Developing next generation applications and data centres requiring next generation security and application security.
- Managing and securing the proliferation of BYOD and mobile devices.
- Mitigating risk and compliance across the organization.
- Developing highly functioning IT organizations while reducing costs.

For more information about TÜV Rheinland, please visit www.tuv.com

For more information about OpenSky, please visit www.openskycorp.com

Contact Details

Nigel Stanley

MSc (Lond.) CEng MIEEE MIET MBCS

Practice Director – Cyber Security

Email: nstanley@openskyuk.com

www.openskyuk.com

Fetcham Park House, Lower Road, Leatherhead, Surrey, KT22 9HD

United Kingdom

References

[1] US Food and Drug Administration, “Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication,” 31 July 2015. [Online]. Available: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm. [Accessed 16 October 2015].

[2] Department of Homeland Security, “Advisory (ICSA-15-161-01),” 12 June 2015. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-15-161-01. [Accessed 16 October 2015].

[3] I. Thomson, “This hospital drug pump can be hacked over a network – and the US FDA is freaking out,” 1 August 2015. [Online]. Available: http://www.theregister.co.uk/2015/08/01/fda_hospitals_hospira_pump_hacks/. [Accessed 16 October 2015].

[4] ICS-CERT, “Advisory (ICSMA-16-089-01),” [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSMA-16-089-01. [Accessed 27th September 2016].

[5] European Commission, “Digital Agenda for Europe,” 28th July 2015. [Online]. Available: http://ec.europa.eu/digital-agenda/cybersecurity. [Accessed 20th October 2015].

[6] U.S. Food and Drug Administration, “Cybersecurity,” U.S. Food and Drug Administration, 22nd September 2015. [Online]. Available: http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm. [Accessed 20th October 2015].