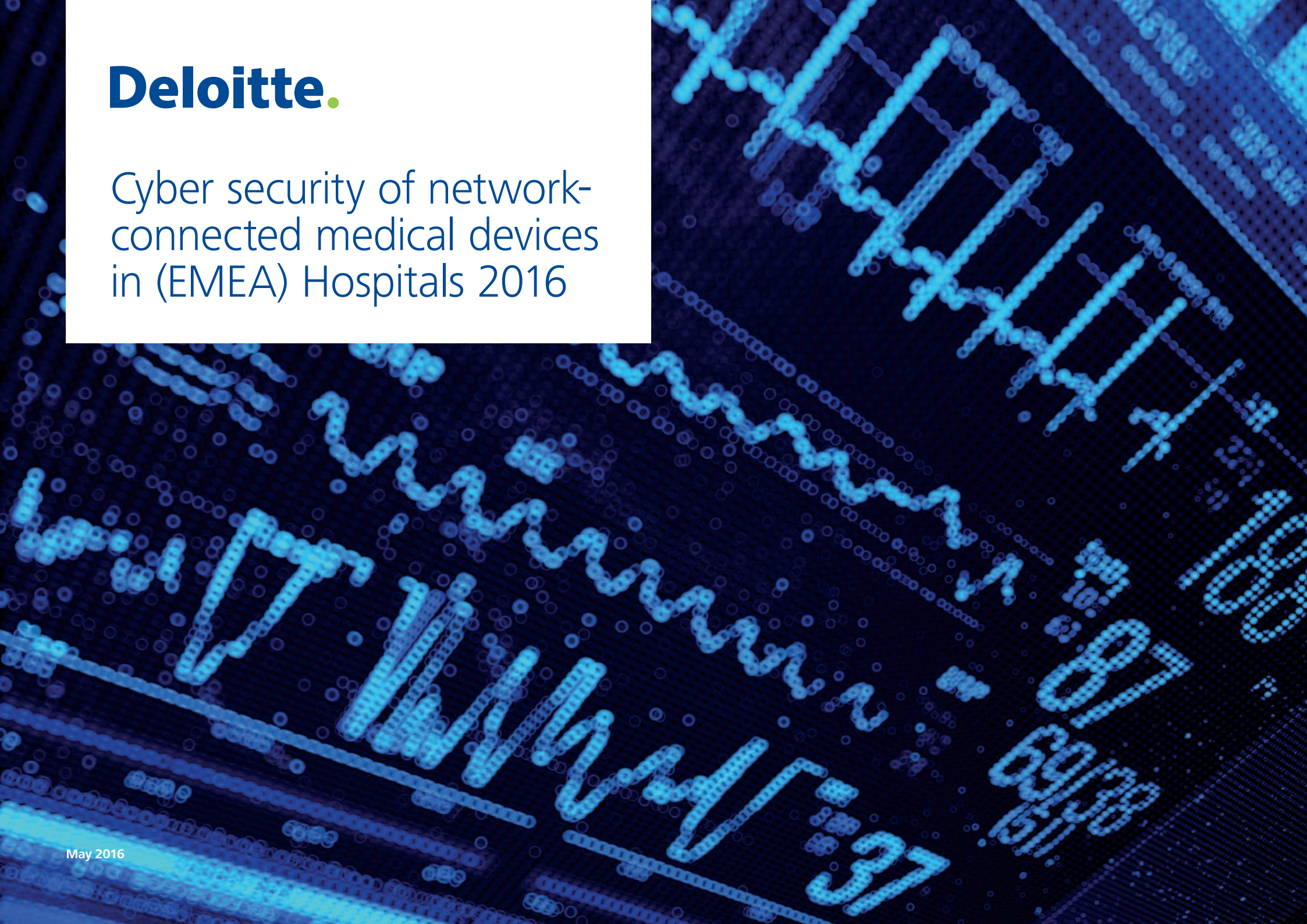
Deloitte.

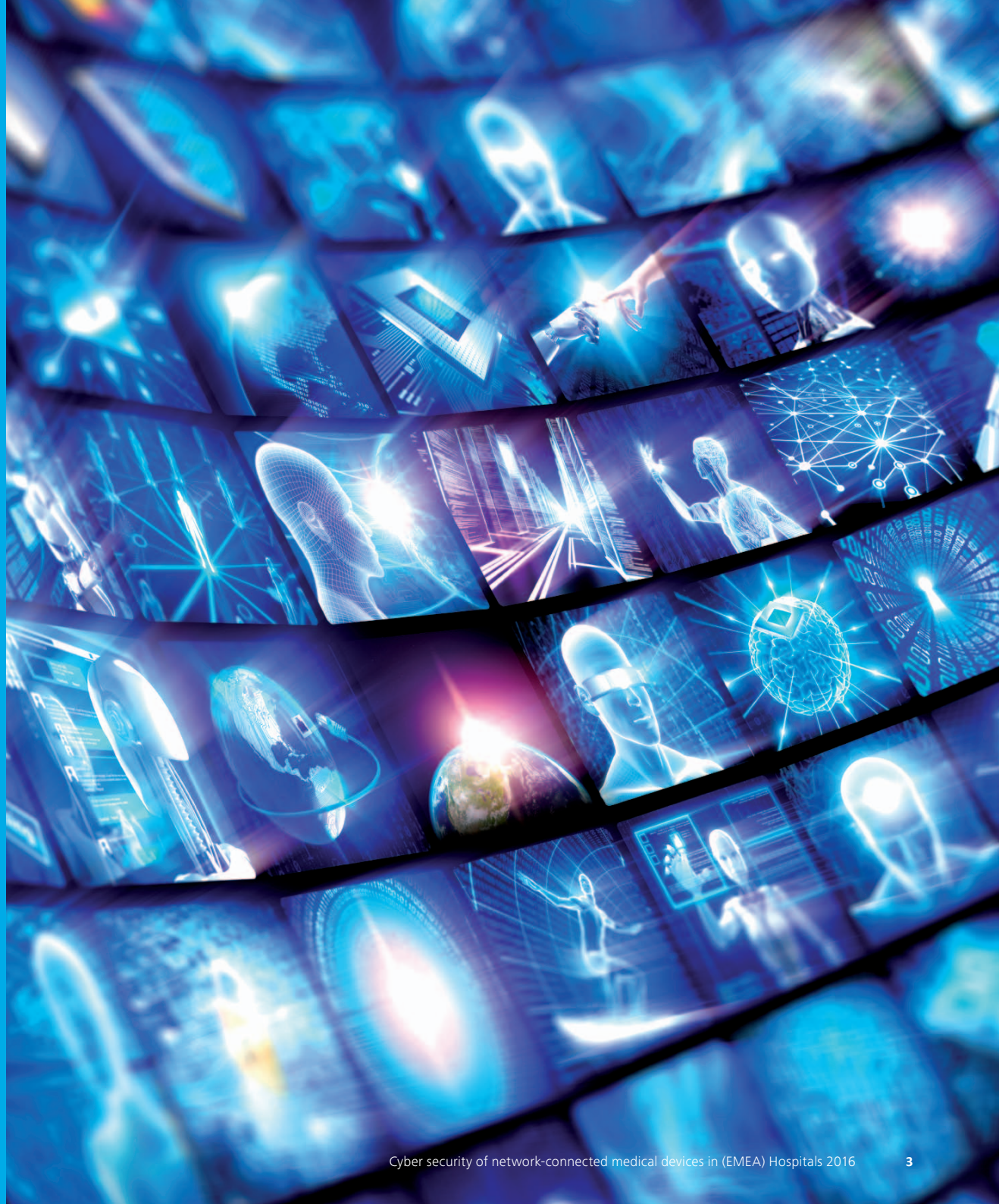
Cyber security of network-connected medical devices in (EMEA) Hospitals 2016



May 2016

Contents

Medical Device Security Survey 2016



Executive Summary

Weaknesses in medical device security attracted media attention in 2015 when hacker conferences exposed vulnerabilities in devices such as infusion pumps, EEG scanners and narcotic equipment.[1, 2, 3, 4] Researchers have since demonstrated, using a honeypot, that hackers would indeed attack exposed medical devices.[5] Last year the European Union Agency for Network and Information Security (ENISA) facilitated workshops to stress the importance of medical device security.[6] Meanwhile the USA Food & Drug Administration (FDA) has issued guidance on the security of medical devices[7] and the Council of the European Union has proposed legislation to enforce medical device security.[8] More recently a grassroots computer security organization, the 'I Am The Cavalry' movement, called for a Hippocratic Oath for connected medical devices.[9]

In response to the 2015 cyber security report on connected medical devices[10] we decided to conduct interviews in various countries. Between March and December 2015 we therefore interviewed people from 24 hospitals in 9 different countries (Switzerland, Israel, Germany, Luxemburg, Netherlands, Czech Republic, Italy, South Africa and Greece).

Although awareness of medical device security has increased and initiatives have been taken to improve the cyber security of these devices, our research demonstrates that more steps can be taken to improve the situation. Our three key takeaways during the interviews are:

- More than half the hospitals stated that they had medical devices with default/ hard-coded passwords;
- Almost half the hospitals did not assess their medical devices for compliance with forthcoming privacy legislation;
- Three of the 24 hospitals had experienced malware incidents last year.

When default passwords on devices are not changed it is easy for attackers to gain unauthorized access to a device and potentially compromise patient privacy or even patient safety. While during a malware infection the integrity and functioning of medical devices cannot be guaranteed. Nevertheless, we continue to believe that innovating is essential for companies and hence worth the risk because the health benefits that new solutions could provide prevail over the examples of security incidents known to have occurred. More attention needs, therefore, to be paid to medical device security and privacy if we want to innovate faster and more, if we want society to readily adopt new medical technologies and if we generally want to improve the quality of devices (and specifically the data they contain). Cyber hygiene of medical devices should, therefore, be our aim.

Approach & Methodology

Under the promise of strict anonymity, we interviewed people from 24 hospitals in 9 different countries. These hospitals differed in size, location and type (general/academic). To ensure consistency within the interviews we used a standardized questionnaire and held several preparatory discussions with the interviewers. Over a period of nine months we interviewed various hospital professionals (doctors, security officers, chiefs of medical technology & IT) working with medical devices and/or IT on a regular basis. We subsequently reviewed the questionnaires of the interviews to ensure the respondents' answers had been correctly transcribed.

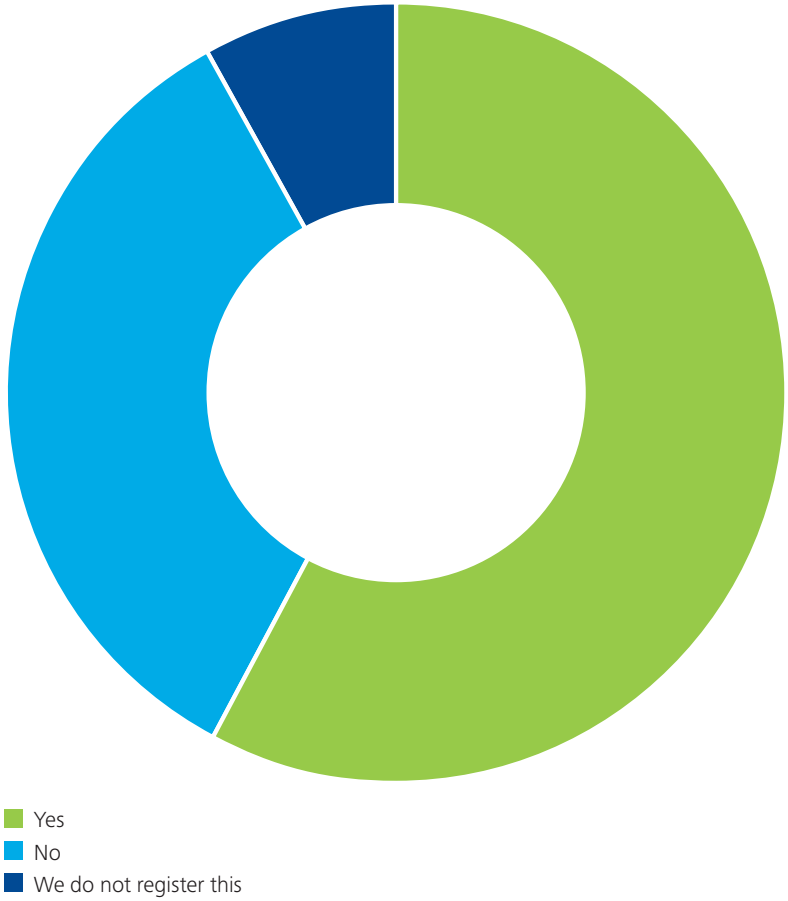
Hard-coded and default passwords could facilitate attacks on medical devices

More than half the hospitals stated that they had medical devices with default/hard-coded passwords.

The risk of having default passwords on connected medical equipment is that this makes it easy for unauthorized attackers (such as hackers) to obtain access to the device and to influence its functioning and/or read patient data. Passwords can often be guessed or found in a publicly available product manual.

The solution is for default passwords in a system to be changed in line with security standards. Manufacturers must ensure that passwords can be changed or even enforce such changes, based on good practices such as those suggested by the OWASP IoT Project[11]. Hospitals should demand the opportunity to change passwords. If this is not possible, monitoring solutions combined with network segregation should be applied as a second-best option.

Do you have medical devices with a default (or hard coded) password in your hospital?



Limited availability of secure connections

Five of the 24 hospitals stated that most of their devices used a secure connection.

The risk of unencrypted connections varies, depending on the network architecture. If no additional control measures are implemented, an attacker may be able to access all the data on a hospital network. Data confidentiality and integrity cannot then be ensured. This could ultimately result in a risk to patient safety (e.g. if false data are entered into a communication stream) or leakage of patient data.

If a device does not have encrypted connections, an alternative would be to introduce surrounding control mechanisms such as monitoring solutions, network segregation or network access controls.

What percentage of your medical devices use an encrypted connection to send data to back-end systems or other medical devices?

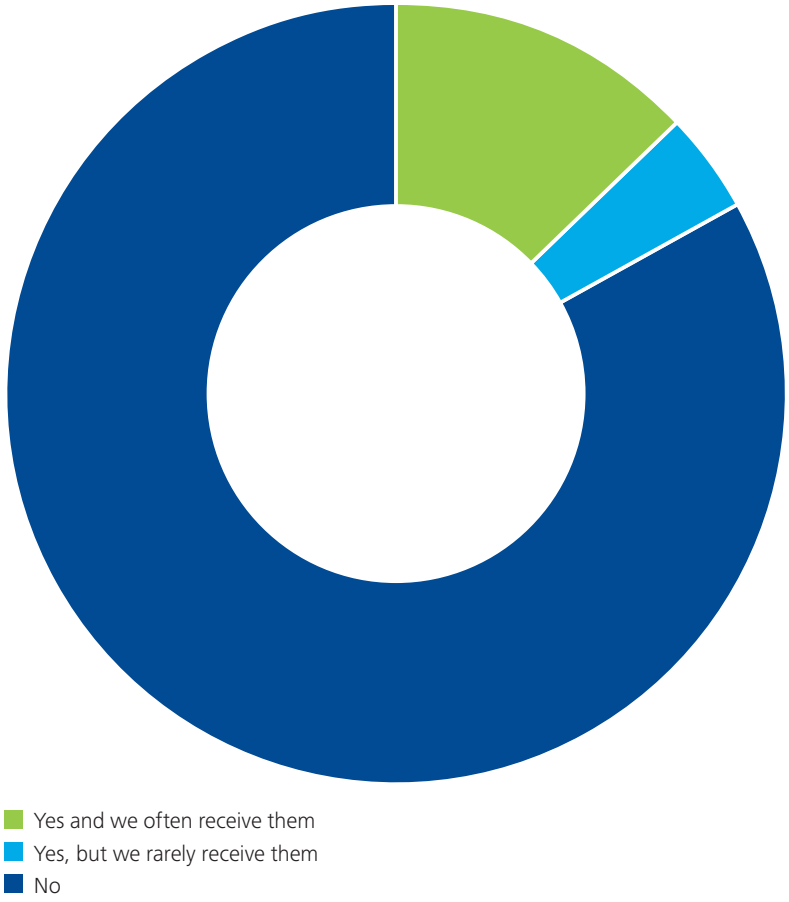
Transparency-enforcing tools not always used

More than three quarters of the hospitals did not request the MDS2 form before purchasing medical devices.

The Medical Device Security Manufacturer Disclosure Statement (MDS2) [12] summarizes devices' cyber security risks. Hospitals could use these forms to determine which devices require additional control mechanisms (such as monitoring solutions) and which devices are most resilient.

The risk of not using the MDS2 form is that essential security requirements will not be considered when new medical devices are acquired.

Do you actively ask for a MDS2 form (Medical Device Security Manufacturer Disclosure Statement) before purchasing a medical device?



Medical devices are often not assessed against new privacy legislation

Almost half the hospitals did not assess their medical devices for compliance with new privacy legislation (e.g. the EU's General Data Protection Regulation or Data Breach Notification legislation), while a few stated that they had devices where compliance could be difficult to achieve owing to the lack of certain functionalities (e.g. a lack of adequate security controls).

The risk of not assessing medical devices for compliance with privacy legislation is that a hospital may be unaware of its failure to comply. This could ultimately result in fines being imposed on the hospital or in damage to its reputation if patients lose trust in the hospital because of its failure to respect their privacy.

When acquiring a medical device, hospitals should assess whether it meets their privacy requirements.

As an additional benefit of ensuring privacy, hospitals may be able to obtain more usable research data. These data could then form the basis for new treatments and innovations to improve patients' health.

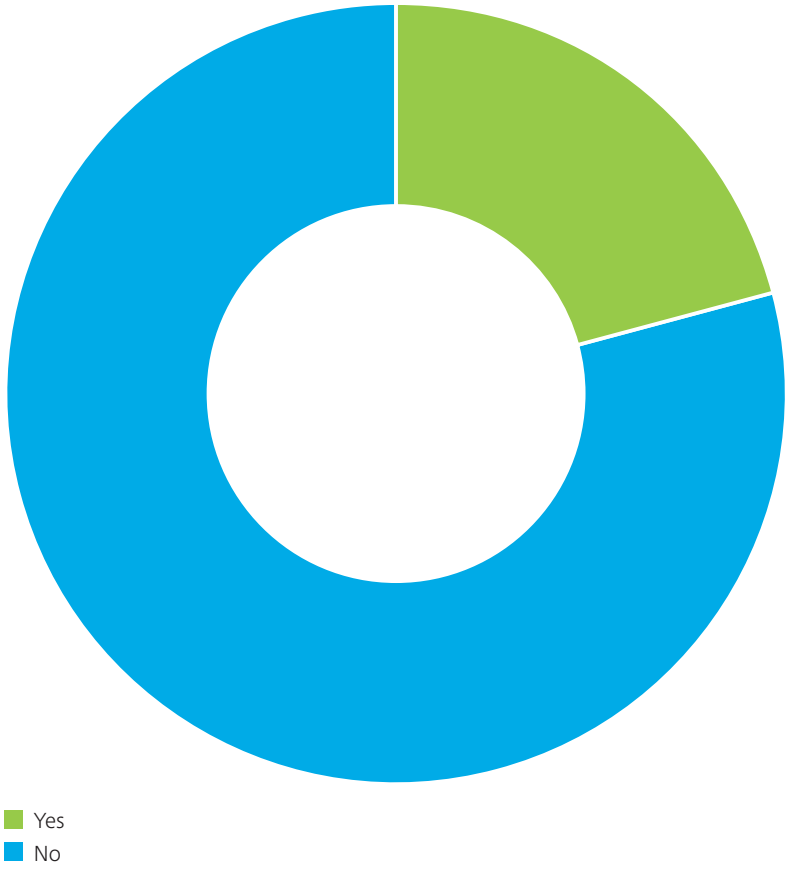
Considering personal data, is your medical equipment ready for new European privacy legislation?

Medical device security often lacks dedicated policy

Five of the 24 hospitals stated that they had an explicit information security policy in place for medical devices.

Having a clear policy on medical device cyber security is important because it sets standards for dealing with cyber security, while also assigning accountability and enabling alignment between different departments. Our survey found that Medical Technology and IT were sometimes in two entirely different departments and that responsibilities for medical devices' cyber security were consequently unclear. Explicit policy is needed to clarify these issues.

Do you have a cyber security policy for the cyber security of connected medical devices?



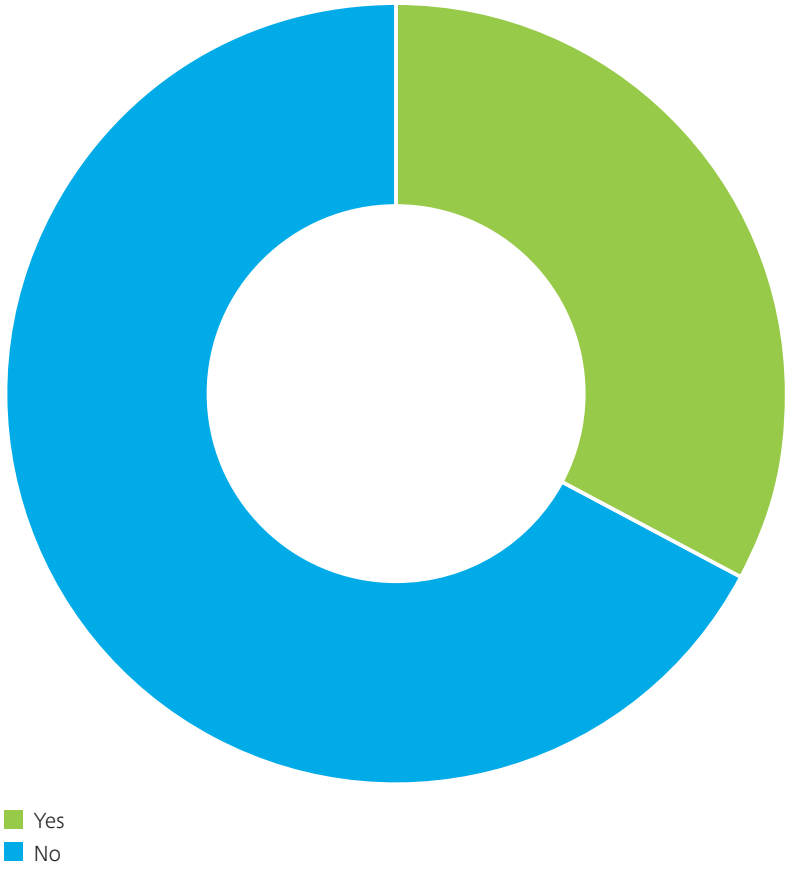
Vulnerability management often not performed

Two third of the hospitals stated that they did not monitor medical devices for known/ published vulnerabilities.

The risk of not monitoring vulnerabilities is that a hospital could be unaware that its medical devices are vulnerable. This in turn could result in data breaches and/or compromise safety.

Hospitals should regard vulnerability management of their devices in the same way as basic hygiene and maintenance of traditional equipment.

Do you check if your hospital uses specific equipment when a vulnerability of a medical device is published (for example on ICS-CERT, or a security conference)?



Malware on medical devices remains troublesome

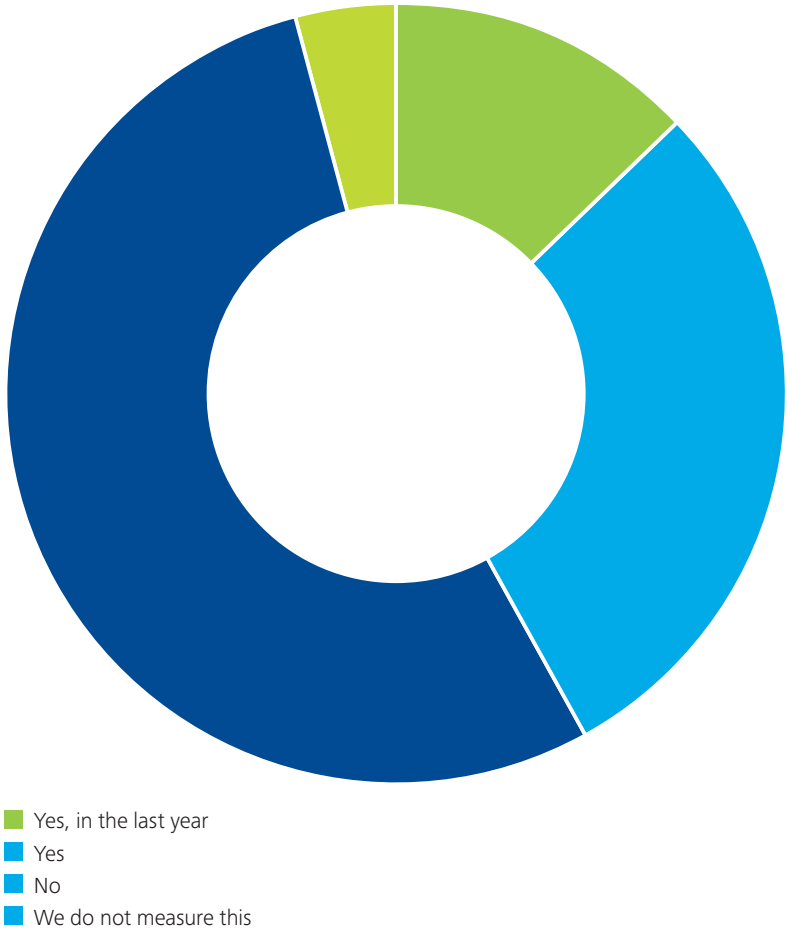
Three of the hospitals interviewed had experienced a malware / computer virus in the previous year, while one hospital did not record such incidents. Malware represent a major risk.

The integrity and functioning of medical devices cannot be guaranteed in the event of such an infection. Some malware may cause performance issues that can endanger devices' availability and therefore the hospital's operational processes – and, hence, its treatments – may be jeopardized if they solely depend on those devices.

Installing virus scanners on medical devices is not always a solution as not all equipment supports this, while hospitals are not always authorized to install software on devices they have purchased. If, however, software is permitted to be installed on medical devices, installing anti-virus software or a white-listing solution may be beneficial.

Other solutions in addition to network segmentation may include Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Security Information & Event Management (SIEM).

Did a malware / computer virus infection, infect medical devices in your hospital?



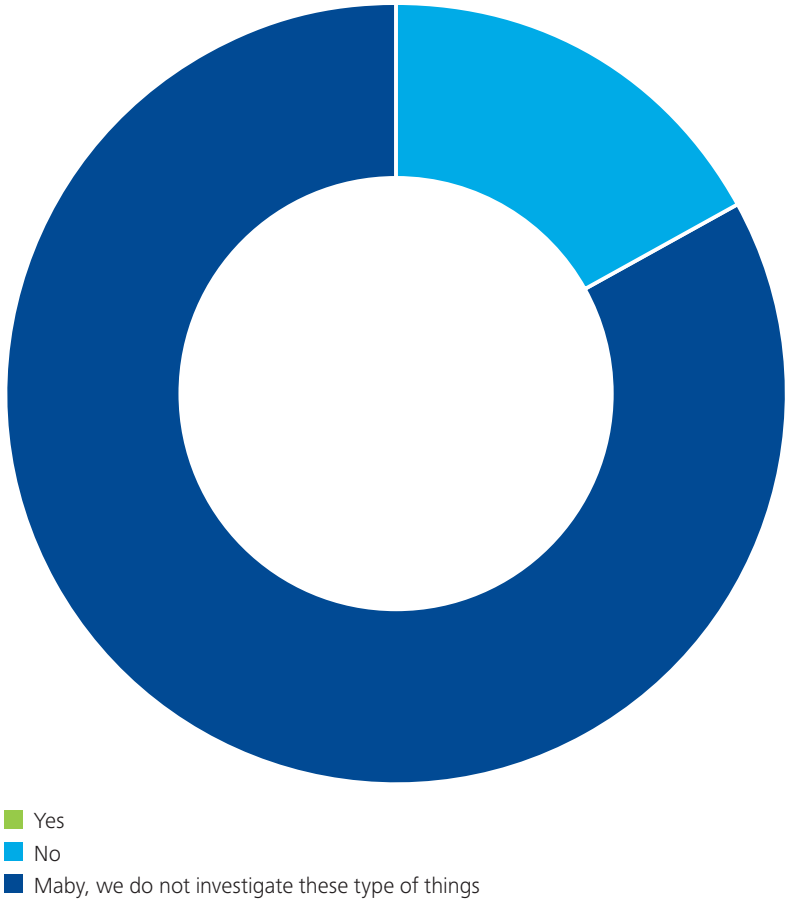
No known patient safety incidents. But not always investigated

Almost a fifth of the hospitals interviewed stated that patient safety issues relating to cyber security incidents in medical devices were never investigated.

Although we did not receive any indications during the interviews that any patient safety incidents attributable to cyber security had occurred, it is important to monitor and investigate incidents that could have been triggered in this way as research has demonstrated that such incidents are possible.

Investigating cyber security incidents for their potential impact on patient safety could provide a basis for research, while also increasing medical device security and promoting continuous improvements within an organization. Such investigations will also boost overall awareness of basic cyber security hygiene.

Did you ever had a medical device (security) incident that resulted (or almost resulted) in patient injury or worse, the dead of a patient?



Conclusion

During the interviews with hospital staff we observed that the awareness of medical device security has improved. Many of the interviewees had thought about medical device security and recognized some of the challenges.

At an operational level, however, there is still room for improvement. Account should consequently be taken of the following observations when dealing with medical device security and privacy:

- More than half the hospitals stated that they had medical devices with default/ hard-coded passwords;
- Almost half the hospitals did not assess their medical devices for compliance with forthcoming privacy legislation, while a few even stated that they had devices that could never be compliant owing to specific functionalities;
- Five of the 24 hospitals stated that most of their devices used a secure connection, while the others stated that only a few or none of their devices used a secure connection;
- Over three quarters of the hospitals did not request the MDS2 form before acquiring medical devices;
- Five of the 24 hospitals stated that they had an explicit information security policy in place for medical devices, while the other 19 stated that they did not;
- Over three quarters of the hospitals stated that cyber security incidents relating to medical devices had never resulted in a safety issue, while almost a fifth stated that safety issues relating to cyber security incidents of medical devices were never investigated;
- Around two thirds of the hospitals stated that they did not monitor medical devices for known/published vulnerabilities;
- Three of the 24 hospitals had experienced malware incidents last year, while one did not record such incidents.

Privacy and security should be factored in to new medical devices from the start. This will enable the countless opportunities offered by new technologies to be used safely.

Recommendations

During the interviews we noticed a number of good practices which are ordered by three categories beneath:

Secure

- Hospitals could work together to jointly demand and increase cyber security in medical devices; in effect, therefore, asking for security and privacy by design;
- Privacy should become an integral part of medical technology strategy and an enabler of medical device innovation;
- One person could be designated responsible for medical equipment's as well as IT cyber security;
- Use of network segmentation, anti-virus (white listing) solutions and Network Access Controls (NAC);
- Removable media to be checked before they are allowed to be used on medical devices.

Vigilant

- As with basic hygiene, cyber security is everyone's business. Continuous awareness of the link between cyber security and the safety of medical devices is, therefore, vital;
- Hospitals could actively chase vendors/manufacturers to obtain the required information on device security and demand new functionalities enabling them to work securely;
- Need for continual assessment of the threat/risk landscape so as to improve the situation (assessment can be based on ISO 80001).

Resilient

- Use of Security Operations Center (SOC) supported by Security Information and Event Management (SIEM);
- Monitor medical device anomalies and combine this with incident response capabilities [13];
- Incorporate Medical Device Security scenario's within crisis management trainings and procedures;

References

[1] *https://ics-cert.us-cert.gov/advisories/ICSA-15-337-02*

[2] *http://www.spiegel.de/spiegel/vorab/hacker-kapert-narkosegeraet-a-1047197.html*

[3] *http://www.theregister.co.uk/2015/10/13/brain_waves_security/*

[4] *http://www.slideshare.net/Shakacon/medical-devices-passwords-to-pwnage-by-scott-erven*

[5] *http://www.theregister.co.uk/2015/09/29/thousands_of_directly_hackable_hospital_devices_found_exposed/?mt=1443524487087*

[6] *https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-healthcare*

[7] *http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf*

[8] *http://data.consilium.europa.eu/doc/document/ST-12040-2015-ADD-1/en/pdf*

[9] *https://www.iamthecavalry.org/2016/01/19/i-am-the-cavalry-proposes-hippocratic-oath-for-connected-medical-devices/*

[10] *http://www2.deloitte.com/nl/nl/pages/risk/articles/the-cybersecurity-of-network-connected-medical-devices-in-the-netherlands.html*

[11] *https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization / https://www.owasp.org/index.php/Use_of_hard-coded_password /*

[12] *http://www.himss.org/resourcelibrary/MDS2*

[13] *https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-deloitte-cyber-risk-pov-secure-vigilant-resilient.pdf*

Thanks

We would never have been able to perform this research without the hospitals' support. We would therefore like to extend our warmest thanks to everyone involved. The report would also not have been possible without the efforts of:

- Marko van Zwam (NL)
- Derk Wieringa (NL)
- Marrit Plat (NL)
- Niek Ijzinga (NL)
- Jan-Jan Lowijs (NL)
- Jeroen Slobbe (NL)
- Dimitrios Vosikas (GR)
- Ioannis Diveris (GR)
- Fabio Bonanni (IT)
- Federica Innocenti (IT)
- Marco Eggerling (CH)
- Lance McGrath (CH)
- Sebastian Renker (D)
- Fabian Mihailowitsch (D)
- Sven Kreiter (D)
- Peter Wirnsperger (D)
- Ismael Cisse (LU)
- Stephane Hurtaud (LU)
- Gabriela Naiwirtova (CZ)
- Lior Kalev (IL)
- Asaf Reshef (IL)
- Asaf Servi (IL)
- JJ Gericke (SA)
- Cathy Ann Gibson (SA)
- Daniela Vaglietti (SA)
- Henry Peens (SA)
- Tiaan van Schalkwyk (SA)

Medical Device Security

Secure - Vigilant - Resilient

The Edge
Gustav Mahlerlaan 2970
1081 LA Amsterdam

Ir. Jeroen Slobbe
Tel: +31 88 288 2753
E-mail: jslobbe@deloitte.nl