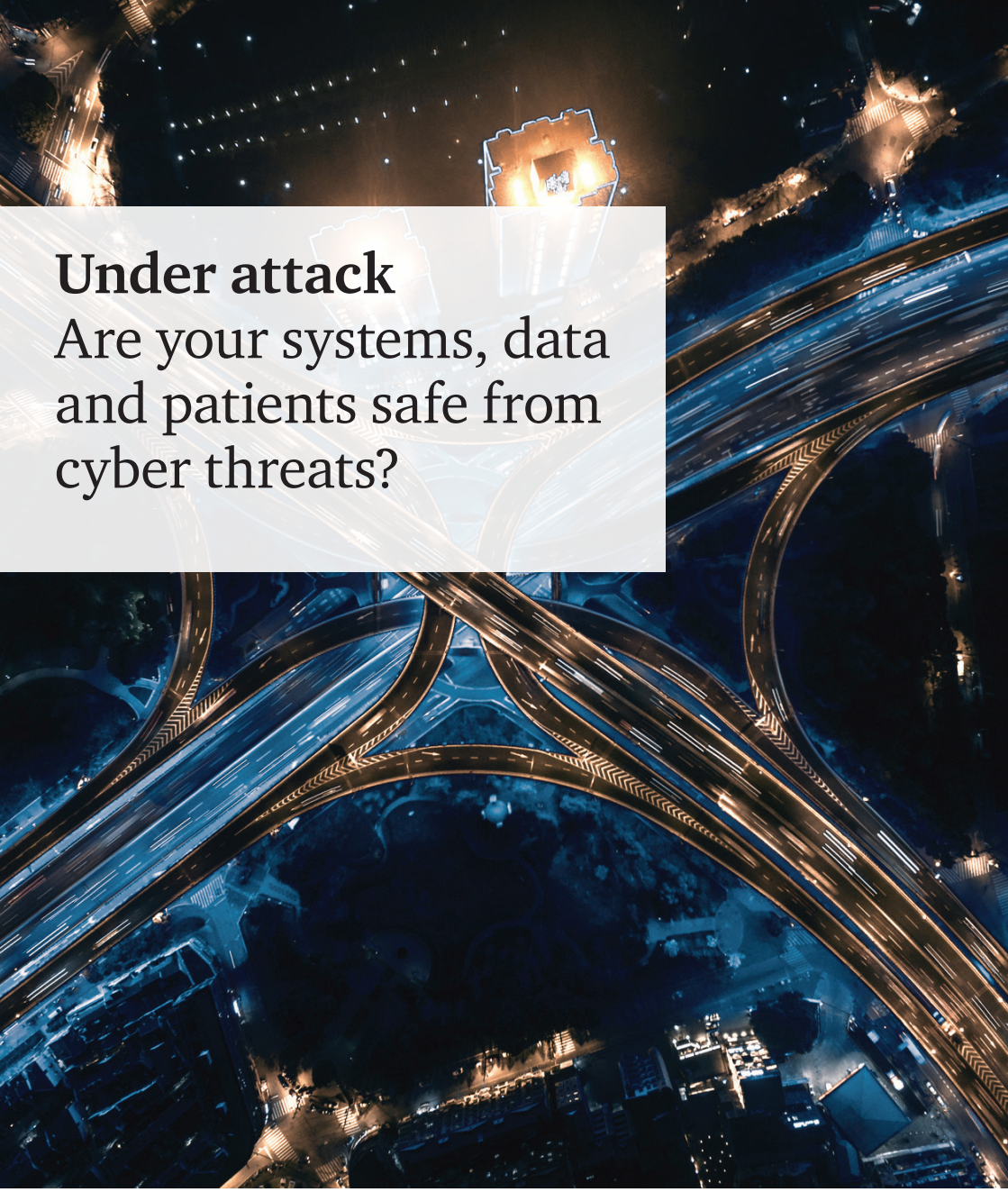
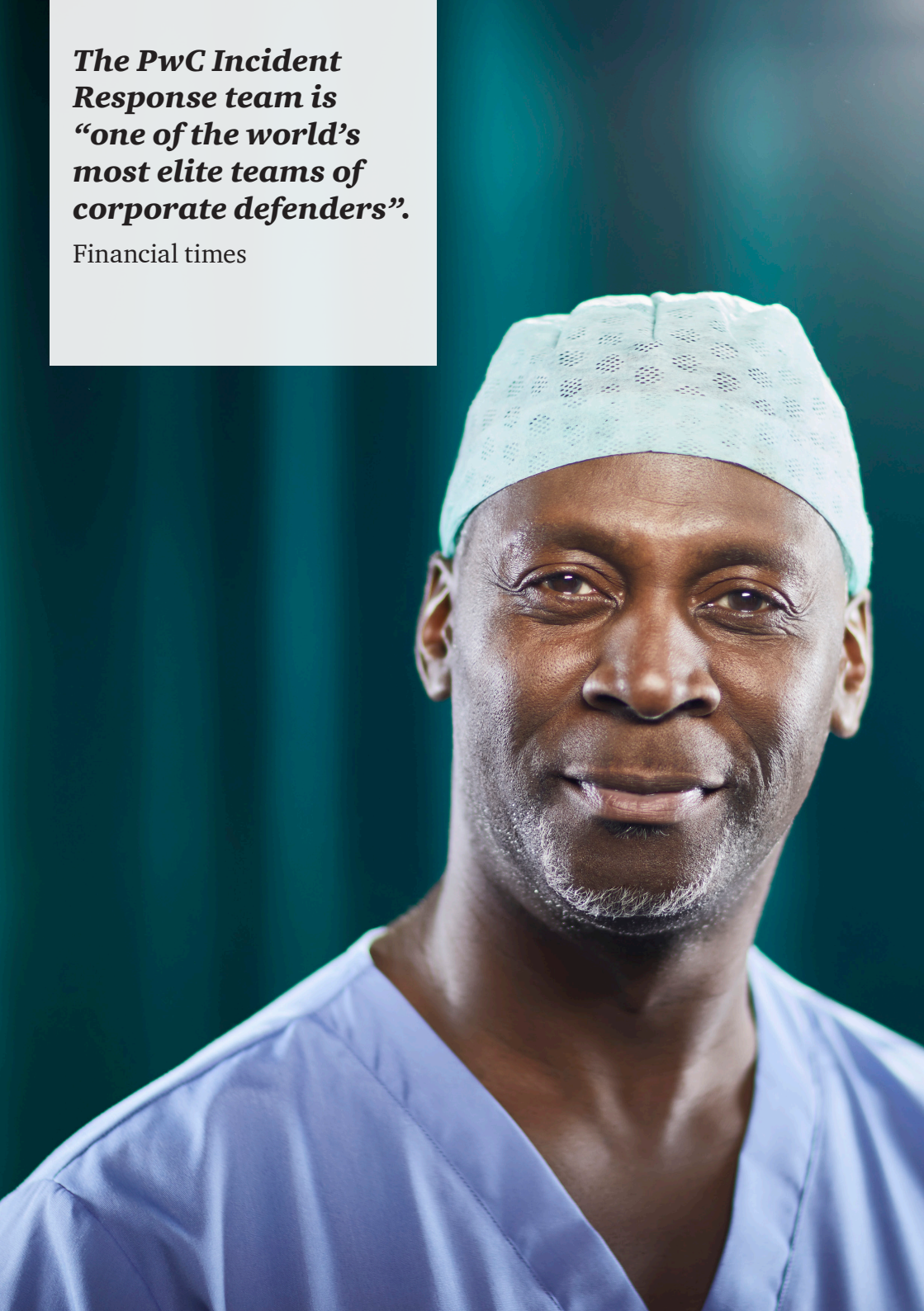


Under attack

Are your systems, data and patients safe from cyber threats?

pwc

www.pwc.co.uk



The PwC Incident Response team is "one of the world's most elite teams of corporate defenders".

Financial times

What cyber threats does the healthcare sector face?

The value of patient data

There is no doubt that the increased use of technology and data have the power to improve health outcomes, transform the quality of provision and help reduce costs for all types of healthcare organisations.

But as confidential data is increasingly stored and accessed on digital devices and equipment – for example, operational systems – embedded devices and consumer technologies, there will inevitably also be a greater risk that the security of this data may be compromised. Additionally, the move towards wearable wireless-connected devices like heart monitors, pacemakers and automatic infusion pumps to track and maintain patients' health exacerbate the risk.

As such technologies become more widespread, security is struggling to keep pace – potentially putting not just patients' data at risk, but their lives. Penetration tests have shown it's possible to gain access to these embedded devices and make life-threatening changes such as altering the pulse rate on a pacemaker, re-programming the doses delivered by an infusion pump or even switching a device off completely.

Attacks within the sector are on the increase. Criminals have realised the value of patient data and are using it as a way of stealing identities.

Recent research shows that of all cyber incidents noted, data breaches are by far the most common, dwarfing rates of all other cyber events – credit card numbers and medical information are the most commonly compromised pieces of information.1

This means public and private health organisations and those in the pharma and life sciences sector underestimate cyber risks at their peril. Each healthcare organisation is responsible for managing their own risks and every health organisation must understand its level of liability and responsibility for data security and privacy in order to ensure compliance, effectively manage future breaches and improve the level of care to patients.

Consider these facts:

1. Personal healthcare records are 10 times more valuable than financial data when sold on the 'dark web'.
2. Cyber security budgets remain severely constrained across health, especially within the NHS.
3. The latest *'Global State of Information Security Survey 2016'* highlighted that some of the biggest healthcare breaches in history were reported over the past year.

What is the landscape in the UK?

Rules and regulations

Alongside the growing threats from adversaries ranging from organised criminals to state-sponsored attackers, healthcare providers, commissioners and connected sectors are also facing a 'perfect storm' of legislation and regulation. This includes new data security standards following the Care Quality Commission (CQC) Data Security Review 2016, the third Caldicott Report and the enforcement of the General Data Protection Regulation from May 2018, which imposes a much more onerous regime and is backed by a significant financial penalty and compensation regime for breaches.

Key implications of the regulatory landscape

Caldicott

- Data security must have same external assurance rigour as financial and clinical systems and processes.
- Qualified data security expertise available to advise every Board.
- Need for focussed Information Governance training for ALL staff.

GDPR

- New consent model that must be transparent and explicit.
- Mandatory breach notification for patients.
- Requirement for Data Privacy Impact Assessments.
- Requirements for qualified data protection officers with practical experience (an estimated 28,000 will be needed).
- A fearsome regime for non-compliance.

We are fast approaching the most significant data privacy legal change in a generation – the EU General Data Protection Regulation. This tough new law has been passed and compliance will be required by Spring 2018, following a two year implementation window. While this window should give entities time to prepare, we are seeing many entities simply not properly engaged in the process and are at risk of non-compliance.

To ensure compliance, providers, Clinical Commissioning Groups (CCGs), hospital trusts and healthcare organisations need to act now as the failure to comply could result in fines of up to 4% of the entity's annual worldwide turnover as well as compensation payments and class action lawsuits.

What should healthcare institutions be doing?

Protect what matters most *– it can be difficult to secure everything, so identify and locate your critical and sensitive information assets and enhance security around them.*

Awareness is key *– ensure your people are aware of the risks, trained in cyber security and understand their responsibilities.*

Get the basics right *– out-of-date and unpatched systems can provide an easy route in for attackers.*

Plan for the inevitable *– assess your response through simulations and regular testing, and develop your crisis and technical response plans and policies accordingly. It's better to fail at a simulation than in real life.*

Use the Information Governance Toolkit *provided by NHS Digital (formally HSCIC – the Health and Social Care Information Centre) to ensure privacy and protection.*

It is difficult to protect what you can't see *– proactively monitor and detect for cyber threats and activity across your network, endpoint and log data – and ultimately enhance visibility.*

How we can help

*We are globally recognised as a leader in cyber and information security and have more than **200 cyber professionals** in the UK, including a dedicated team who specialise in healthcare and data privacy. We are proud to offer services that are unique to us: being the only service provider in the market who can provide **end-to-end**, integrated cyber security services and the **only major professional services organisation approved by GCHQ** to deal with sophisticated, targeted cyber attacks against networks of national significance.*

Our approach recognises the multi-faceted nature of cyber security, and draws on specialists in process improvement, value and change management, human resources, forensics, risk, and legal. Our services are designed to provide our clients with the confidence they seek in an ever-changing digital and connected world.

Our teams cover the full range of cyber services whether that be building defences, responding to attacks or navigating the legal and regulatory landscape.

Building defences

Your cyber strategy should be to keep your organisation safe. This requires an approach that is integrated with your operations throughout your organisation. We can help you develop a broader strategic response to cyber risks, strengthen your defences, test your infrastructure and transform your security posture both technically and culturally.

Identifying and responding to attacks

Healthcare organisations are already under attack. We can help you respond to incidents and manage the response to help ensure the loss of data is swiftly contained and technical systems are restored with limited disruption.
Our team can carry out post-incident forensics investigations to help you understand the nature of the breach and how to prevent future attacks.

Legal and regulatory landscape

We assist from cyber security and data protection strategic development through to post-incident regulatory engagement and litigation. Our team are national leaders and have deep insight into the mind of the regulator,
a thorough understanding of the political landscape driving these changes and a genuine familiarity with all aspects of the health sector.

Anna Blackman
Partner, Health Risk Assurance Leader
+44 (0)20 7212 5983
anna.blackman@uk.pwc.com

Yvonne Mowlds
Partner, Health Forensics Leader
+44 (0)20 7804 9436
yvonne.m.mowlds@uk.pwc.com

Stewart Room
Partner, Cyber Security and Data Protection Leader
+44 (0)20 7213 4306
stewart.room@uk.pwc.com

26% *of publicly recorded data breach incidents within the health sector* were due to human error

2/3 of pharma companies *have suffered serious data breaches*

1/4 *have been hacked*

7,255 *NHS data breaches* between 2011 and 2014

Jeremy Hunt's target is to achieve

25% *of smart phone users accessing and updating patient data* by April 2017

By 2020, Internet-connected healthcare products are expected to be worth an estimated

£220bn *globally in economic value*

In 2016 two trusts were fined

£365,000

between them for leaking *information about thousands of NHS staff and hundreds of patients with HIV*

Health industries: our people

Ian Baxter
Partner, Corporate Finance
+44 (0)20 7213 3914

Jo Pisani
Partner, Pharmaceuticals and Life Science Consulting Lead
+44 (0)20 7804 3744

Brian Pomering
Partner, Health Industries Consulting Lead
+44 (0)20 7213 2101

Andrew Packman
Partner, Pharmaceutical and Life Science Sector Lead
+44 (0)18 9552 2104

Health industries

Tomorrow's healthcare today

Healthcare matters to us and it matters to our clients. We all want better healthcare, sooner and the potential is there to make it happen. New technology, new breakthroughs, new ideas. But while there are opportunities, there are challenges too: constrained budgets, an ageing population and an increase in chronic conditions. At PwC we're working with clients to steer a course to success in this new health economy so we help improve healthcare for all. We're working with the NHS, nationally and locally, as well as the private sector and the pharmaceutical and life sciences sector to deliver real, workable solutions to today's challenges. We're delivering transformation and integration projects with patient outcomes at their heart. And we're supporting organisations through testing financial times, often developing bespoke operational and digital systems. We give strategic support to organisations across healthcare and pride ourselves on convening different parts of the system to solve problems. We also bring insight and expertise to healthcare as well as engaging in the public policy debate.

For more information, sign up for our Health Matters blog at: *www.pwc.blogs.com/health_matters*

Quentin Cole
Partner, UK Leader of Government and Health Industries
+44 (0) 2072 126784

Lucy Stapleton
Partner, Pharmaceuticals and Life Sciences Sector Lead
+44 (0) 2078 042629

Andrew McKechnie
Partner, Private Health Sector and Deals Lead
+44 (0) 2072 126327

Rt. Hon. Alan Milburn
Health Industries Oversight Board Chair
+44 (0)20 7212 6784

www.pwc.co.uk

180529-094514-JC-UK