netwrix

5 Steps to Protect PHI and Pass Compliance Audits with Less Effort

Duncan Innes
Public Sector IT Audit & Compliance Specialist
Netwrix Corporation

Russell McDermott
Systems Engineer
Netwrix Corporation

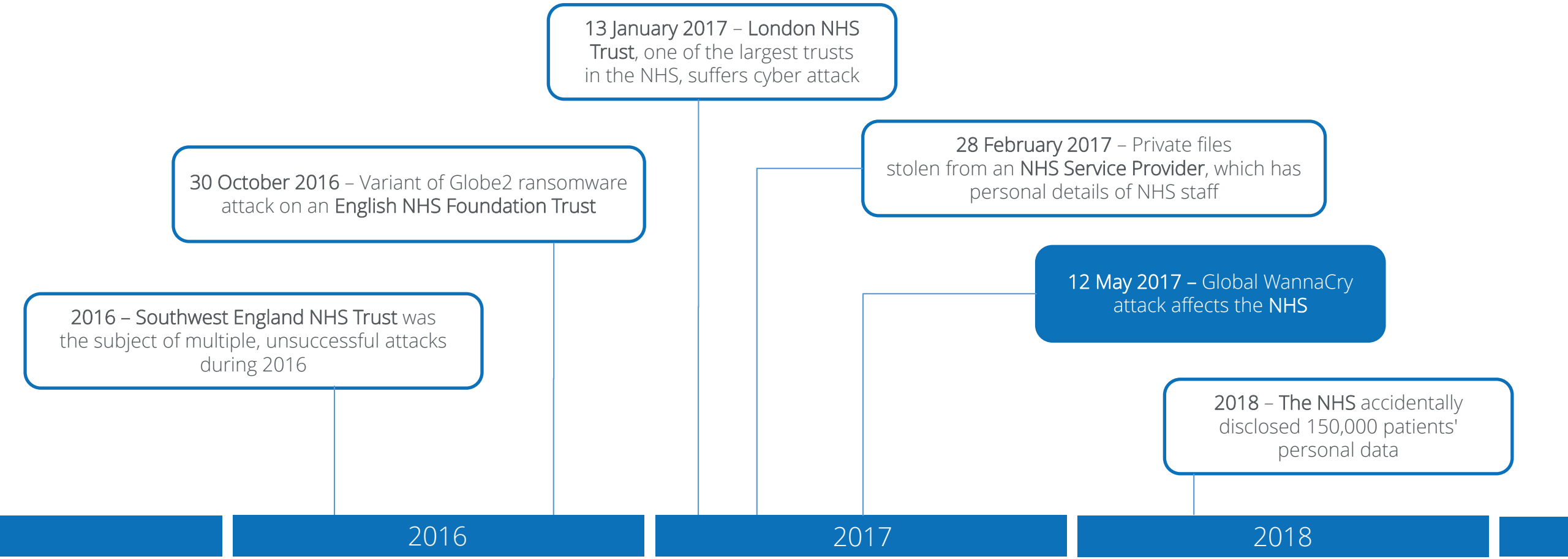
Agenda

- Why you need to worry
- Notorious data breaches
- GDPR compliance: panacea or pain point?
- Go Beyond Compliance
- 5 steps to protect PHI
- Case study: King's College Hospital
- Questions and answers

Why You Need to Worry

- 70 percent of healthcare organisations around the world have experienced a data breach
- PHI and PII command a high value on the shadow markets
- Adhering to compliance requirements doesn't keep all health information safe
- 6 in 10 security breaches in healthcare stem from either malicious or negligent employees
- Organisations invest too much in wrong solutions
- Too much data: no understanding of what's going on

Healthcare Data Breaches



Source: National Audit Office

Perimeter Is Not Helping

- BYOD;
- IoT;
- Interconnectivity;
- More data;
- Cloud – scary move?!
- Insecure devices;
- Vulnerabilities in applications and systems;
- More hackers!
- Ransomware-as-a-service and other easy-to-use hacking tools;
- Intrusion tactics are smarter;
- State-sponsored attacks.

GDPR Compliance

You are obliged to implement controls

- Identity management and access control: to ensure that data is only accessible by personnel that have a business need.
- System configuration control: tracking configuration changes and administrative activities.
- Monitoring of access to data: knowledge of who accessed what data and when and review on a regular basis.
- Data handling and encryption control: protection of data in storage and during transfers.

But does it really help protect the data?

GDPR Compliance: Panacea or Pain Point?

A very brief review:

- Superseded the Data Protection Directive 95/46/EC
- Aims to protect the privacy of individuals in the European Union (EU)
- Gives individuals more control of their personal information processed by companies, and eases law enforcement
- Requires notification in the event of a breach
- Also affects non-European companies that offer goods or services to, or monitor the behavior of, European Union residents
- Fines for non-compliance are tremendous

Why Go “Beyond Compliance”

- **Regulation** and **compliance** will continue to change and evolve - being compliant today does not guarantee you will be compliant in the future
- **Threat actors** will continue to evolve; in reality, they don’t care if you’re compliant or not
- There are always going to be **weak points** in your armour, therefore understanding the risk, and managing it, is key
- Your **staff** are your key asset, and the overriding majority want what is best for the company. However, they are human and will make mistakes, so we need to design with this in mind

5 steps to protect PHI

Conduct risk analysis

Consider threats from insiders and business partners

Enforce security policies and controls; make sure they work properly

Train your employees

Adopt best practices

Why Visibility?

Main reasons to implement a visibility and governance platform:

Case Study

Netwrix Auditor came out on top because it was more thorough and easier to use. It only took under an hour to set up Netwrix. With another solution it took over a week to get it set up and even then it didn't work properly. Netwrix cost us four times less, so it's a huge difference. It wasn't even a close comparison. I'm very pleased with the decision to bring Netwrix Auditor into the King's network. I would give Netwrix 10 out of 10; it meets every single requirement we wanted from it.

King's College Hospital NHS
NHS Foundation Trust

David Sewoke
Head of the ICT Operations
Team King's College Hospital

netwrix

Netwrix Auditor

Demonstration

Netwrix Auditor

A **visibility** platform for **user behavior analysis** and **risk mitigation** that enables control over **changes**, **configurations**, and **access** in hybrid IT environments.

It provides security **intelligence** to identify security holes, **detect** anomalies in user behavior and **investigate** threat patterns in time to **prevent** real damage.

Netwrix Auditor Applications

- Netwrix Auditor for Active Directory
- Netwrix Auditor for Azure AD
- Netwrix Auditor for Exchange
- Netwrix Auditor for Office 365
- Netwrix Auditor for Windows File Servers
- Netwrix Auditor for EMC
- Netwrix Auditor for NetApp
- Netwrix Auditor for SharePoint
- Netwrix Auditor for Oracle Database
- Netwrix Auditor for SQL Server
- Netwrix Auditor for Windows Server
- Netwrix Auditor for VMware

NETWRIX AUDITOR – **Data Discovery and Classification Edition**

Identify, Classify and **Secure Sensitive Data** on Your **File Shares**

Why Do Data Discovery and Classification?

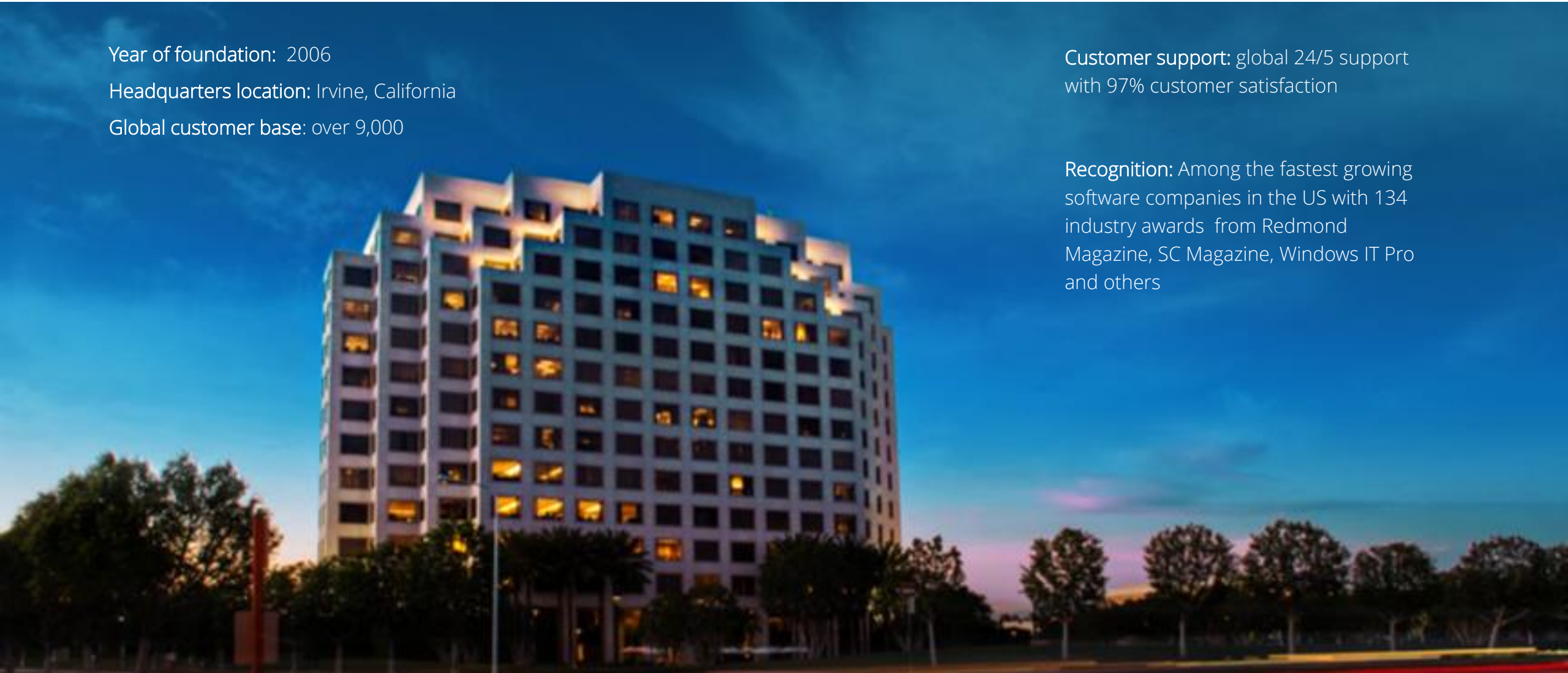
Security of critical data

- What sensitive data do you have?
- Where does this sensitive data reside?
- Who can access, modify and delete it?
- How will it affect your business if this data is leaked, destroyed or improperly altered?

Compliance with regulatory mandates

- GDPR
- PCI
- HIPAA
- SOX

About Netwrix Corporation



Year of foundation: 2006

Headquarters location: Irvine, California

Global customer base: over 9,000

Customer support: global 24/5 support with 97% customer satisfaction

Recognition: Among the fastest growing software companies in the US with 134 industry awards from Redmond Magazine, SC Magazine, Windows IT Pro and others

netwrix

Netwrix UK & Ireland Customers

Netwrix UK & Ireland Customers

Next Steps

Learn how to **prove compliance with ISO/IEC 27001 and GDPR:**

https://try.netwrix.com/healthcare-compliance-uk.html

Check **King's College Hospital** success story:

http://www.netwrix.com/download/CaseStudies/netwrix_customer_success_story_king_college_hospital.pdf

Find out how to **protect the privacy of Electronic Health Records:**

http://www.netwrix.com/download/documents/protect_phi.pdf

Contact Sales to obtain more information netwrix.com/contactsales

Questions?

Thank You!