OSIRIUM

Ransomware and cyber-crime: protecting the NHS

A GUIDE ON

DSPT

COMPLIANCE AND OPTIMISING CYBER SECURITY RESILIENCE

Table of contents

Part 1

The threat to the NHS

In an increasingly digitised world, protecting those services from the disruptive impact of a cyber attack...has never been more important. The cyber security of our health and social care systems underwrites patient safety.

— Lord Markham, Parliamentary Under-Secretary of State in the Department of Health and Social Care.

Introduction

The NHS is a prime target for cyber criminals, with so much highly sensitive data to steal, and it is particularly difficult to protect, with many disparate pieces of infrastructure.

To combat this threat, the NHS announced a new cyber strategy in 2023, emphasising the importance it has for patient safety.

It also updated and strengthened its compliance requirements - the DSP Toolkit - and published a new policy mandating Multi-Factor Authentication is implemented across all digital systems. The latter places particular requirements on privileged accounts.

The cyber security strategy for health and adult social care sets out a plan to promote cyber resilience across the sector by 2030.

The NHS says protection of devices, services and networks and the information on them from theft or damage - is an essential part of patient care.

Health Minister Lord Markham said: “It’s crucial we’re bolstering the defences of our health and care services. This new strategy will be instrumental to ensure every organisation in health and adult social care is set up to meet the challenges of the future.”

What is the NHS trying to protect?

Devices: diagnostic machines - imaging scanners and systems that let hospitals know which beds are free.

Primary care: including patient booking systems, call and recall facilities, and electronic prescription services.

Adult social care organisations: technologies such as digital care records and acoustic monitoring systems that are enabling more responsive, joined-up care.

In this guide, we will look at:

- Threats posed to the NHS’ cyber security
- What aspects of the NHS are at risk?
- Compliance: the DSP toolkit
- The new MFA policy
- The importance of Privileged Access
- Ransomware and endpoint protection
- Third party access and back ups
- How Osirium can help

Part 2

The Data Security and Protection (DSP) Toolkit

All organisations that have access to NHS patient data and systems must use this Toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

— *NHS Digital*

NHS Digital

The Data Security and Protection (DSP) Toolkit is an online tool that enables relevant organisations to measure their performance against the data security and information governance requirements mandated by the Department of Health and Social Care (DHSC). Such organisations are required to carry out self-assessments of their compliance against the assertions and evidence contained within the DSP Toolkit.

Self-assessments must be completed annually and twice a year for those in category 1 and 2 – NHS Trusts and "Arm's length" bodies such clinical commissioning groups. Compliance is required of all service providers ranging from local authorities to GP practices and business partners.

More on the DSP Toolkit

- Turn to Section 5 for more information about the importance of privileged access in the DSPT.
- Turn to Section 12 (appendix) of this guide for a full table with more details.

Key Challenges for DSP Compliance

There are a number of common challenges that DSP brings, as summarised in this table below:

Common challenge	How does privileged access security help?
Governance of user credentials including adherence to password policies and removing access when no longer needed.	The heart of Privileged Access Security (PAS) is Privileged Access Management (PAM) which is the central visibility and control hub for all privileged access to shared devices, systems, and data. With this single point of control, policies can be implemented, enforced and audited.
Ensuring staff and partners can only access the systems they need and having control over what they do with that access.	As above, PAM provides that central control point to ensure users only have access to the systems they need. It also provides the option to watch, in real-time, what staff and partners are doing with the option to shut down any inappropriate sessions. It also becomes the ultimate audit trail of who did what and when for auditing purposes or incident investigation.
Providing evidence for DSP compliance.	When the organisation spans many sites, there are hundreds of different servers, devices, applications and services to manage, collecting the required evidence to support a DSP audit is difficult and time-consuming. Using PAM as the gateway to all those systems and being confident it ensures policy compliance simplifies the process and reduces the load on the IT team for each assessment.

Part 3

How vulnerable is the NHS?

> *The scale of impact - both direct and indirect - from a cyber attack on the health and social care sector is potentially huge.*
>
> — *Source: Policy Paper: a cyber resilient health and adult social care system in England: cyber security strategy to 2030*

Threats and attacks

In England and internationally, there have been various instances where cyber attacks have disrupted the running of services, at times with significant financial consequences. The huge impact that an attack can have is emphasised by these stats:

There are estimated daily:

950,000
General practice appointments

45,000
Major A&E department attendances

137,000
Imaging events

Although our cyber defences have improved over the past years and especially since WannaCry in 2017, we know we still have further to go."

— Phil Huggins, National Chief Information Security Officer

2017 WannaCry ransomware attack

- Absolutely devastated NHS systems and crippled their business operations.
- According to NHS England, the WannaCry ransomware affected at least 80 out of the 236 trusts across England - either infected by the ransomware or turned off their devices or systems as a precaution.
- Also infected: further 603 primary care and other NHS organisations with 595 GP practices.
- The attack led to disruption in at least 34% of trusts in England, although the Department and NHS England do not know the full extent of the disruption
- 34 trusts were infected and locked out of devices (of which, 25 were acute trusts)

2022 NHS ransomware attack:

- A ransomware attack on a software supplier provides software for various parts of the NHS hit the NHS across the UK
- The attack on the morning of August 4th caused widespread outages across the NHS.
- It affected services including patient referrals, ambulance dispatch, out-of-hours appointment bookings, mental health services and emergency prescriptions.

2021 HSE attack:

- The Health Service Executive (HSE) in Ireland, suffered a major ransomware attack which caused 80% of the HSE IT environment to become encrypted.

Part 4

The rising ransomware threat

The most significant cyber threat the sector faces is ransomware.

— *Source: Policy Paper: a cyber resilient health and adult social care system in England: cyber security strategy to 2030*

The rise of ransomware

Ransomware attacks have increased substantially in recent times. Increasingly, those attacks are abusing admin credentials to help their propagation around corporate networks. They also target the systems critical for protection and recovery. It's a smart move: if backups are corrupted or deleted, paying the ransom demand to decrypt the data becomes a more attractive option for the victim. Unfortunately, paying a ransom doesn't always solve the problem. Even having the decryption key isn't a guarantee the data can be recovered. Some studies have shown that a company that pays a ransom is more likely to be victims of further attacks

Description:
Ransomware attacks, used by criminals to damage and disrupt anorganisation's network, have become commonplace. Malicious software hijacks a computer, locking out users and encrypting files while the 'bad actor' demands a ransom payment. Osirium research suggests 79% of UK businesses have suffered such an attack.

The problem with endpoints

Most cyber attacks start with staff in the organisation. In many organisations, too many users have the power to install applications or update their Windows desktops, exposing the business to major threats, such as ransomware. That's because they have local admin rights. Removing local admin rights radically reduces the risk of security breaches. So cyber security strategies should focus on this, first and foremost.

Verizon's latest Data Breach Investigations Report reveals that human error is a contributing factor to four in every five breaches, with staff continuing to be susceptible to social engineering attacks and privileged access misuse.

OSIRIUM **EPM**

How can an Endpoint Privilege Management solution (EPM) help?

- Easily and safely removes local admin rights wherever required
- Radically reduces the risks of a ransomware attack
- Reduces the burden on overly busy IT help desks

Part 5

The importance of privileged access

Privileged accounts provide elevated, often unrestricted access to an organisation's underlying information systems and technology, making them rich targets for malicious actors.

— *NIST*

Privileged account abuse

The dangers of privileged access misuse are highlighted as a critical concern in the new NHS cyber strategy.

Privileged account abuse is one of the most critical security challenges that face all organisations today.

What's the problem?

Every IT infrastructure is managed by these privileged users – users granted elevated control through accessing privileged accounts to ensure that the uptime, performance, resources and security of the infrastructure meets the needs of the organisation.

Administrator accounts are particularly sensitive due to their elevated privileges when used with IT systems. In terms of the NHS, accounts can be used to exfiltrate sensitive patient data, interrupt services, or make it easy for ransomware attacks to strike.

What's an example in the NHS?

A new team member joins a GP practice's team. The traditional process is to send a request to an IT Service Desk to provision the user's accounts, which may be in 4 or 5 systems, including Active Directory (AD), Office365, EMIS, and/or clinical systems. This places significant demand on the Service Desk and may introduce a delay before that new team member can start work.

When someone leaves, the reverse must happen: all those accounts must be removed quickly which is not always possible due to service demand spikes.

In some situations, if a user needed an elevated account, a manual process would be used to create a temporary login and then remove the account when no longer needed. Across the integrated care system group, such account management tasks are happening every day. It's often an urgent demand for the IT Service Desk which impacts productivity at the GP practice and opens potential security risks.

What does the DSPT say about privileged access?

Managing Privileged access already features prominently in the DSP guidelines, which tell NHS IT leaders to "closely manage privileged user access to networks and information systems supporting the essential service".

A significant element is monitoring and managing how user accounts are created, maintained, and removed when no longer needed, especially those with elevated privileges.

CASE STUDY

"Privileged Access Management is very much about protecting your crown jewels. You put a lot of effort into designing access control policies and locking down platforms, but the key to all of that is your administrative credentials. If you don't maintain strict control over your high-level accounts then what's the point of all your other security controls?"

Jonathan Freedman, Head of Technology and Security at London law firm Howard Kennedy

Read the case study

Six key points about privileged access in the DSPT

1. IT leaders must ensure that "logs, including privileged account use, are kept securely and only accessible to appropriate personnel".
2. These should be "stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate".
3. What are described as "unnecessary user accounts", must be disabled or removed.
4. "privileged user access is also removed when no longer required or appropriate".
5. Former employees, guest and other unnecessary accounts are routinely and promptly removed or disabled from internal workstations, Active Directory domains and other user directories.
6. IT staff must consider the extent to which third parties are being granted privileged access and if it's being limited to a set time to "mitigate the danger of security breaches". That's because it's hard to ensure third parties have the same of security hygiene and also to prevent them sharing credentials.

The insider threat

The new NHS Cyber Strategy highlights the potential 'insider threat' posed within the health and social care sector by staff or contractors.

It raises the threat of "people working in or near to the health and social care sector seeking to misuse their privileged access."

Whilst attention is often focused on hackers and external threats, the risk from, for example, a disgruntled employee or someone with third party access, can easily be overlooked.

In such examples, someone may try to do damage or steal patient information before leaving the organisation.

Part 6

The dangers of third-party access

> *Ransomware and other cyber crime is also a threat to third party suppliers, an attack on whom can cause as much or more damage and disruption as an attack directly on a health or care organisation.*

— Source: Policy Paper: a cyber resilient health and adult social care system in England: cyber security strategy to 2030

What is the problem with third-party access?

Every organisation depends on close relationships with suppliers, partners, and outsourced staff.

Working closely with these third parties, whilst bringing many benefits, adds a lot of risks, unless key security measures are in place, with the right controls and monitoring.

To do their work, they typically need access to corporate IT systems.

But what organisations need to secure remote access without exposing the keys to their kingdom. Uncontrolled access to privileged accounts by third parties (such as the many NHS contractors) leaves an organisation utterly vulnerable to data leaks and breaches, ultimately causing irreversible damage to both the organisation, its' reputation and its trust with patients.

It's hard to ensure that all these vendors have the same level of security hygiene as is used internally. It's also hard to ensure that the people who have been granted access don't share their credentials.

To stay safe, it's vital to take measures such as separating them from credentials, not allow VPN access, use multi-factor authentication, and record sessions.

OSIRIUM

How can Osirium help?

PAM software can allow partners or suppliers to safely access internal systems without needing complex remote access infrastructure while increasing visibility with real-time session monitoring.

Part 7

The threat to back-up systems

Online backups are at significant risk because, in the event of a ransomware attack, the backup system faithfully takes copies of the infected data and thus renders the backups useless.

— *David Guyatt, Executive Chairman at Osirium*

Backup systems and backups themselves are being targeted by ransomware attackers. Once an attack occurs, assuming you're not going to pay the ransom, and even if you do pay the ransom, you're not guaranteed to get your data back because there are bugs in the code. So even if you get the decryption key, that may not work.

The essential route to recovery is to restore from a backup, so therefore cyber criminals aim to delete the backups, encrypt them, and stop them from being recovered.

Indeed, the NCSC made specific recommendations about protecting backups to NHS Trusts in 2021, as part of serious concerns about the NHS being a target for cyber attackers. The NCSC said they should pay extra attention to protecting backup systems. And on the back of that, NHS Digital made budget available to invest in privileged access management specifically for backup systems - £5,000 per Trust.

The NCSC says: ""Ensure you create offline backups that are kept separate, in a different location (ideally offsite), from your network and systems, or in a cloud service designed for this purpose, as ransomware actively targets backups to increase the likelihood of payment."

What does DSPT instruct about backups?

- Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.
- Backups are routinely tested to make sure that data and information can be restored
- Your organisation's backups are kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose.

Part 8

Multi-factor authentication

Multi-factor authentication is widely recognised as one of the most effective ways to protect data and accounts from unauthorised access.

— *NHS Digital*

Multi-factor authentication

In September 2023, NHS Digital introduced a new mandate for all NHS bodies to enforce MFA protection on all digital systems.

The directive puts a particular emphasis on accounts with privileged access.

Organisations must demonstrate to The National Chief Information Security Officer that they have achieved full compliance by 30 June 2024.

NHS Digital states that organisations must enforce MFA on:

1. All remote user access to all systems
2. All privileged user access to externally-hosted systems

On top of that it "should enforce MFA on all privileged user access to all other systems".

What does NHS Digital say?

"This policy will ensure that MFA is used on digital systems throughout the health sector, with particular requirements on accounts that are remotely accessible or have privileged access to systems.

"Industry research suggests that MFA can prevent 99.9% of account compromise attacks, and MFA is widely considered by cyber security authorities globally to be one of the most important controls that any organisation can deploy. Its use in the NHS will help protect patient data and organisations' capability to deliver patient care."

Which bodies does it apply to?

NHS trusts and foundation trusts

- Integrated care boards
- Arm's length bodies of the Department of Health and Social Care
- Commissioning support units in NHS England
- Operators of essential services for the health sector in England as designated under the NIS Regulations

OSIRIUM

How can Osirium help?

Osirium PAM includes time-based one-time passwords (TOTP) for multi-factor authentication (MFA) and also supports external authentication through RADIUS with major IAM solutions to reduce the risk of third-party accounts being shared.

Single Sign On (SSO) is performed by injecting the required admin credentials for the target system by PAM. This means passwords are never sent down to the client, thereby removing the possibility that sniffing memory, or looking at command strings within the process tree, will ever reveal a password.

Part 9

How are NHS trusts protecting themselves?

Osirium has helped us close the technology gap bringing control and oversight into an area where previously our only control was one of mutual trust.

— *Mark Grant, IT Infrastructure Operations Manager at NHS Lanarkshire*

Real life case studies - in brief

More than 50 NHS bodies trust Osirium to help protect them from ransomware attacks. Here, we look at two examples in brief.

NHS Lanarkshire

- Third largest NHS authority in Scotland
- Cares for over 655,000 people.
- With three main acute care sites, 15 community hospitals, over 90 GP surgeries, and more than 14,500 staff, the trust's IT department is responsible for a complex and disparate IT estate.
- With over 14,000 Windows endpoints, 900+ servers, over 200 admin accounts, and more than 300 service accounts across their systems, it was impossible to safely manage all accounts and devices manually.
- Needed to improve security for managing privileged access - both internal staff and many third-party suppliers that have access to internal systems.
- Lacked visibility and control of supplier access using these powerful accounts was identified as a significant risk.

Read the case study in full

The NHS Midlands and Lancashire Commissioning Support Unit (MLCSU)

- Provides wide-ranging IT support services to Integrated Care Systems (ICS) groups across the Midlands, Lancashire and North-West England.
- Unlike Acute Trusts, which typically focus on a few large sites (usually hospitals), primary care is much more diverse.
- Provides a broad range of services to approximately 200 organisations and their services range from desktop deployment and clinical systems to Cyber Security.
- Needed support to help clients conform to DSP requirements
- Was tasked with transforming IT Service Delivery for GP practices
- Key challenge was reducing the load on the IT Service Desk

Read the case study in full

Part 10

How can Osirium help?

It's been a really good relationship with Osirium, and nothing was too much trouble. They've been very responsive and supportive.

— Glenn Hollywell, Senior Project Manager, NHS MLCSU Cyber Security Team

Every IT team is under pressure so can ill-afford time spent on collecting and submitting the required items of evidence, hence the urgent need for tools that can reduce or remove any manual effort.

That's where modern privileged access management (PAM) and automation is the solution. If the systems are in place to ensure policy compliance, they are being used and those tools can provide the necessary audit information, then DSPT submissions should be straightforward.

DSP compliance should not be just a box-ticking exercise. If done well, PAM and automation not only provides security for systems and data but can be a positive contribution to reducing manual effort, reducing cost, and improving service in everyday operations. For example:

Osirium PAM can allow partners or suppliers to safely access internal systems without needing complex remote access infrastructure while increasing visibility with real-time session monitoring.

Admins have faster access to the servers and systems they need through the Osirium PAM client – rather than having to find the right device in a list of hundreds or thousands, they only see the devices they are permitted to use. They can search for relevance devices (e.g. "Firewall in Manchester") and access credentials are injected by PAM so they're never exposed or shared.

Risk is reduced, time is saved, and they can get on with their work.

The "MAP Server" in Osirium PAM, allows legacy applications to be accessed via a browser on any workstation or laptop, allowing the number of old, perhaps out of support systems, to be greatly reduced.

Osirium EPM can help NHS bodies tackle the tricky issue of local admin rights, and thereby radically reduce the risks of ransomware attacks, whilst also maintaining productivity for staff and avoiding adding to the burden of the IT help desks.

Osirium Privileged Process Automation (PPA) can be used to simplify management tasks so they can be safely delegated to IT help desk agents or end users (for example, regular tasks such as recertifying who has access to which systems).

Find out more about how we can protect your organisation by booking a demo, giving us a call, or requesting a call back via email.

Call
+ 44 (0) 118 324 2444

Chat
www.osirium.com

Email
info@osirium.com

Part 11
Appendix

DSPT requirements in detail

It's crucial we're bolstering the defences of our health and care services.

— Lord Markham, Parliamentary Under-Secretary of State in the Department of Health and Social Care.

Assertion	Evidence ref	Evidence text	How can Osirium help?
Organisation assures good management and maintenance of identity and access control for it's networks and information systems.	4.2.3	Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity.	PAM provides a central audit point for all privileged access to shared systems, databases, and network devices.
	4.2.4	Unnecessary user accounts are removed or disabled	Removing accounts can be an automated process in PPA as part of a standard "leaver's process." With access to privileged access managed by PAM, removing a user's access is a simple task in one system rather than the time- consuming and error-prone manual process of updating each system separately.
All staff understand that their activities on IT systems will be monitored and recorded for security purposes.	4.3.2	Are users, systems and (where appropriate) devices always identified and authenticated prior to being permitted access to information or systems?	Access to systems can only be made via the PAM system as the credentials are only held within PAM. Users must prove their identity before being able to use PAM. That proof may require Multi-Factor Authentication (MFA).
	4.3.3	Have all staff been notified that their system use could be monitored?	All or selected sessions can be recorded via the PAM system. When a recorded session starts, the user can be warned that the session is being recorded.
You closely manage privileged user access to networks and information systems supporting the essential service.	4.4.1	Has the Head of IT, or equivalent, confirmed that IT administrator activities are logged, and those logs are only accessible to appropriate personnel?	The PAM system maintains full audit trails of all sessions. Auditor can be granted limited access to review the logs as needed.

Assertion	Evidence ref	Evidence text	How can Osirium help?
You closely manage privileged user access to networks and information systems supporting the essential service.	4.4.2	The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high- risk functions, in particular reading email and web browsing.	Protected servers should only have the applications needed to perform their work (i.e. no web browser or email client). PAM can further restrict access to specific applications via the “MAP Server”. For maximum protection, automation can be used to ensure only specific functions are performed and the user cannot do anything they should not.
	4.4.3	The organisation only allows privileged access to be initiated from devices owned and managed by your organisation	Access to Osirium PAM can be managed rather than configuring access on every device, system or service.
You ensure your passwords are suitable for the information you are protecting.	4.5.2	Technical controls enforce password policy and mitigate against password- guessing attacks.	Privileged credentials managed by PAM can have policies and lifecycles enforced, for example, password complexity or rotation frequency. Because this is a machine-driven activity, it does not fall into the traps of poor password choice when humans must change passwords.
	4.5.3	Multifactor authentication is used wherever technically feasible.	Multi-Factor Authentication via numerous methods can be requirement to prove the user’s identity before gaining access to privileged systems.
	4.5.4	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.	Privileged credential governance ensures passwords are changed when onboarding new systems and future updates follow prescribed policies.

Assertion	Evidence ref	Evidence text	How can Osirium help?
You ensure your passwords are suitable for the information you are protecting. (continued)	4.5.5	Does your organisation grant limited privileged access and third party access only for a limited time period, or is it planning to do so?	PAM allows access to external parties within selected time windows. Access is only granted to approved systems and all third-party access can be recorded.
		Do you have high-strength passwords defined in policy and enforced technically for all users of internet-facing authentication services?	PAM implements complex credential lifecycle policies for access to systems with privileged access.
All networking components have had their default passwords changed.	9.1.1	The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password. planning to do so?	All new devices should have all their accounts managed by Osirium PAM so no default accounts will be left on the devices.
The organisation is protected by a well managed firewall.	9.6.1	Have one or more firewalls (or similar network device) been installed on all the boundaries of the organisation's internal network(s)?	Privileged Automation can be used to quickly and securely manage firewall rules and policies.
	9.6.2	Has the administrative interface used to manage the boundary firewall been configured such that; it is not accessible from the Internet, it requires second factor authentication or is access limited to a specific address?	All shared security systems, such as firewalls, should have all accounts managed by PAM to prevent unauthorised access.
	9.6.4	All inbound firewall rules (other than default deny) are documented with business justification and approval by an authorised individual.	Changes to firewalls can be automated by Osirium PPA to ensure policies are followed. They can include approval steps and full audit trails are maintained all approvals and changes.

About Osirium

Osirium is the UK's innovator in Privileged Access Management. Founded in 2008 and with its HQ in the UK, near Reading, Osirium's management team has been helping thousands of organisations over the past 25 years protect and transform their IT security services.

The Osirium team have intelligently combined the latest generation of cyber security and automation technology to create the world's first, built-for-purpose, Privileged Account management and process automation solution.

Tried and tested by some of the world's biggest brands and public-sector bodies, Osirium helps organisations drive down business risks, operational costs and meet IT compliance needs.

For more information, please visit
https://www.osirium.com