ManageEngine
ADManager Plus

A guide to **user lifecycle management and cyber essentials** in the UK healthcare sector

Table of content

UK healthcare cybersecurity: A critical overview

All UK residents have access to healthcare through the National Health Service (NHS). As one of the largest healthcare providers in the world, it faces significant challenges when it comes to protecting patient information.

The healthcare sector uses a variety of medical devices, and forming integrations between these devices offers significant benefits for patient care and system efficiency. As the healthcare industry goes through a technological shift to include the use of artificial intelligence, wearable devices, and networked medical equipment, so too will new risks be introduced, such as cyberattacks. Cyberattacks on healthcare systems are becoming more frequent and severe, underscoring the urgent need for cybersecurity measures.

However, cyber threats go beyond data breaches. The disruptions they cause can compromise the safety of patients and interrupt the delivery of healthcare. Due to the interconnected nature of healthcare services, a single incident can have a significant impact on the entire system.

These factors demonstrate the importance of cybersecurity investments for the healthcare industry. This includes adopting advanced security technologies, training staff on cyber hygiene, and implementing data protection best practices. A key goal is to make sure that technological advancements in healthcare do not compromise patient privacy or safety.

Common cyber threats faced in the UK's healthcare system

The UK's National Cyber Security Centre (NCSC) defines cyber security as "how individuals and organisations reduce the risk of cyberattack from malicious attempts to damage, disrupt, or gain unauthorised access to computer systems, networks, or devices."

The healthcare sector is one of the prime targets for cybercriminals. This is largely because health records hold substantial value, often up to ten times more than other types of data. This value proposition, coupled with the sector's vulnerabilities, underscores the critical need for robust cybersecurity measures.

Several factors contribute to healthcare systems' vulnerability. For instance, the healthcare sector is notorious for relying on legacy systems, which pose significant risks due to outdated security measures. The absence of essential updates and patches leaves these systems open to attacks, a fact underscored by numerous incidents targeting such outdated infrastructure.

Furthermore, the increasing interconnectivity of medical devices—including patient monitors and electronic health records—while beneficial for patient care, also opens up new avenues for cyber threats. Devices that are insecurely configured or inadequately maintained can become channels for malware.

However, it's not just the technical infrastructure at risk; the human element plays a crucial role in healthcare cybersecurity. Whether through phishing attacks or social engineering tactics, healthcare professionals and administrative staff can compromise patient data. The integrity and privacy of sensitive information are further harmed by insider threats, whether malicious or negligent.

The UK healthcare system faces a plethora of cyber threats, with ransomware, phishing, and insider threats being particularly prevalent. Ransomware attacks, where sensitive data is encrypted and held for ransom, have surged, disrupting healthcare services and endangering patient records. Phishing attempts, often disguised as legitimate communications, trick employees into revealing sensitive information or installing malicious software. Given the vast amounts of patient data it handles, the healthcare industry is a prime target for such exploits.

Insider threats also represent a significant risk, with employees or contractors potentially misusing or mishandling sensitive data. This can lead to unauthorised access, data theft, or even critical infrastructure sabotage.

Addressing these vulnerabilities requires a multi-faceted approach. Beyond just recognising threats, healthcare organisations must actively update and secure their IT infrastructure. This includes ensuring devices are properly maintained and educating staff on cybersecurity.

Regular training sessions can help mitigate human errors, while adopting the latest security technologies can shield against more sophisticated cyber threats. Moreover, healthcare providers must stay vigilant, continuously assessing and updating their cybersecurity strategies to protect patient data and healthcare services from cyber threats.

The 2017 WannaCry ransomware attack on the NHS

The WannaCry cyber attack was the largest to affect the NHS. The WannaCry ransomware affected dozens of NHS facilities on May 12, 2017, bringing them to a standstill for several days.

An overview of WannaCry

The NSA discovered a Microsoft Windows vulnerability known as EternalBlue that WannaCry exploited. A hacking group known as The Shadow Brokers leaked the hacking tool designed to exploit this vulnerability. When combined with a virus that propagates itself and encrypts files, this vulnerability put cybercriminals in control of powerful malware that ended up being known as WannaCry.

WannaCry encrypts files on a computer, rendering them inaccessible. A ransom note is then presented to victims, demanding a cryptocurrency payment to gain access to the decryption key. WannaCry was thwarted in about half a day due to a cybersecurity researcher finding and disabling the ransomware portion of the malware. However, many devices remained encrypted, leaving them inoperable due to a lack of backups.

The NHS attack

WannaCry spread like wildfire throughout the world, infecting unpatched and outdated systems—hitting the NHS particularly hard. As a result:

- Around 200,000 devices were affected worldwide, with nearly 70,000 of those devices belonging to the NHS.
- A total of 80 NHS trusts, 603 primary care organisations, and 595 general practitioners were affected. Due to the inaccessibility of patient records, non-priority surgeries were delayed and patient appointments were cancelled at many facilities.
- Despite NHS claims that no ransom was paid, an estimated $92 million was lost due to the interruption of service.
- Despite no patient data being compromised, the breach raised serious concerns about future security risks.

What made the NHS vulnerable?

The NHS was an easy target for WannaCry due to several factors:

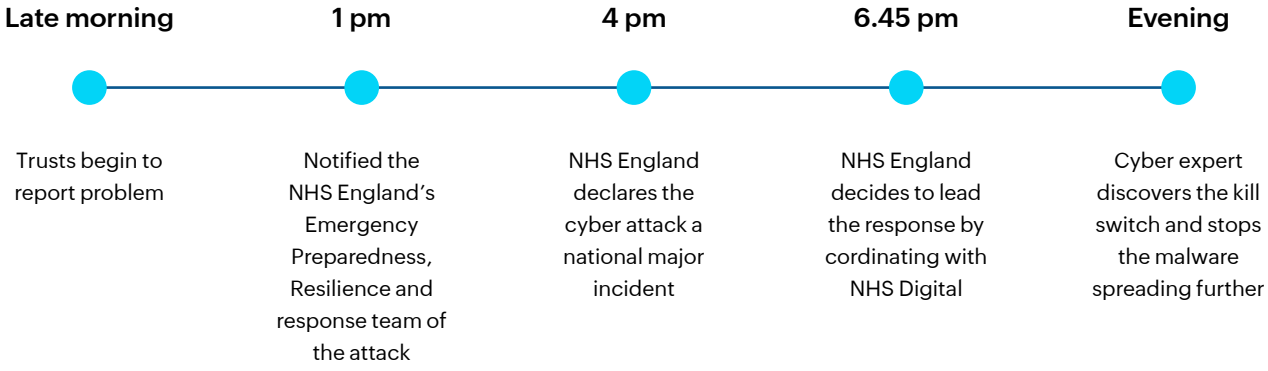
- NHS systems ran on outdated operating systems no longer supported by Microsoft, such as Windows XP.
- It was ill-prepared for an attack of this magnitude despite earlier warnings and fewer cybersecurity incidents.
- As with many public health systems, the NHS faced budgetary constraints, which sometimes meant IT and cybersecurity were not prioritised.
- Since the ransomware spread over the internet, including the N3—a broadband network that connects all NHS sites in England—a properly managed firewall facing the internet would have protected them.

Observations and lessons

The WannaCry incident served as a wake-up call for organisations around the world, it emphasised the importance of:

- Regularly updating and patching systems to fix known vulnerabilities.
- Implementing backups and disaster recovery plans for organisations.
- Ensuring service delivery and patient safety, while also providing adequate resources and budget for cybersecurity.

The WannaCry attack on the NHS 12 May



Healthcare security: The potential impact of these risks

Healthcare cybersecurity breaches can result in significant financial, reputational, and operational losses. Depending on the severity of the breach, financial costs can vary from responding to the incident to restoring systems and paying legal expenses. The reputation of healthcare organisations also takes a hit, leading to a decrease in patient trust.

Failure to adhere to data protection laws—such as the Data Protection Act (DPA) or the General Data Protection Regulation (GDPR)—can result in large fines, adding to the financial burden of a cybersecurity breach.

The most critical impact, however, is on patient safety. Cyberattacks like the WannaCry ransomware have demonstrated how medical services can be disrupted. Hospitals were forced to turn away patients or delay essential medical procedures, which negatively affected patient health.

Security breaches go beyond monetary loss and regulatory fines; they directly compromise patient safety and undermine public confidence. Cybersecurity measures are essential for protecting healthcare services and patient information.

Financial losses and regulatory penalties are not the only consequences of cybersecurity breaches in healthcare. Patient safety and public trust are also compromised. It is imperative to ensure healthcare services and patient data integrity, confidentiality, and availability through robust cybersecurity measures.

The healthcare sector in the UK has faced several cybersecurity challenges, which have led to critical insights into the protection and continuity of sensitive patient data. These incidences underscore the importance of a multifaceted cybersecurity approach that incorporates both technical and procedural components.

Lessons from cyberattacks

The first line of defence is a robust security infrastructure. To prevent breaches and safeguard patient information, advanced threat detection systems, encryption technologies, and secure network architectures are crucial. The human element, however, cannot be overlooked. A comprehensive cybersecurity training program prepares healthcare workers to identify phishing attempts, protect sensitive data, and respond to security incidents effectively. In this way, optimal technological defences are ensured.

The importance of continuous improvement through vulnerability assessments and patch management cannot be overstated, especially when it comes to legacy software and interconnected medical devices. In addition to fulfilling a legal obligation, DPA and GDPR compliance reinforces patient trust.

Healthcare organisations can detect, contain, and mitigate cybersecurity incidents swiftly by proactively establishing and routinely updating incident response plans. Doing so underscores the importance of a comprehensive cybersecurity strategy by minimising the impact on patient care and operations.

Risk assessments are essential for healthcare organisations to identify vulnerabilities and fortify their defences against cyber threats. Additionally, patient care and data security must be prioritised when focusing on mitigation efforts. Security protocols such as firewalls, intrusion detection systems, and encryption protocols are necessary for preventing unauthorised access to networks. Endpoint security solutions, such as antivirus software and encryption, protect devices against malware. Data and systems that contain sensitive information are protected by strong access controls and multi-factor authentication.

Cybersecurity incident management is made more effective and timely if healthcare staff is educated about best practices and common threats. Finally, maintaining patient trust and privacy requires compliance with data protection regulations and industry standards.

These practices can significantly improve the cybersecurity posture of healthcare organisations in the UK. This ensures the integrity of healthcare services and the protection of patient data. A secure healthcare environment that is resilient to evolving cyber threats is built upon a comprehensive approach that balances technological advances with staff training and regulatory compliance.

How Bedforeshire Hospitals ensured cyber resilience

Bedfordshire Hospitals NHS Foundation Trust is a foundation trust of the NHS that serves 1.3 million patients with over 8,000 employees.

They faced the following critical problems:

- **Asset visibility and patch management:** Lacking visibility into its IT assets, Bedfordshire Hospitals faced difficulties managing patches, which resulted in missed patches and inadequate tracking.
- **Management and auditing:** Using Microsoft Management Console and PowerShell was time-consuming and administratively intensive, lacking automation.
- **User account management:** Staying on top of user account management—such as managing stale and disabled accounts, creating bulk accounts, and managing account lockouts and password resets—posed challenges for Bedfordshire Hospitals.
- **Compliance and security:** Monitoring unauthorised access to patient records was a concern due to the sensitive nature of patient information, so Bedfordshire Hospitals needed robust auditing capabilities.
- **Integration and user support:** Finding a solution that integrated seamlessly with the hospitals' existing systems and provided effective user support, including on-site support, was essential.

The problem

- Healthcare delivery was hindered by these issues. The WannaCry ransomware attack exposed and highlighted the lack of visibility over IT assets as a primary cybersecurity concern. These assets had patchable vulnerabilities, but patch management was inadequate due to a reliance on Microsoft Windows Server Update Services (WSUS). The process led to untracked and missing patches—a critical flaw in an environment where data security is paramount.
- The management and auditing of Active Directory (AD) was also a significant challenge. In addition, the IT team relied heavily on Microsoft Management Console and PowerShell scripts, which were time-consuming and difficult to maintain. The manual process of managing and auditing AD resulted in a high administrative burden and inefficiency.
- Another concern is the management of user accounts. Managing stale and disabled accounts was a challenge for the team. There were inefficiencies and increased workloads for IT staff due to the lack of automation in the process of creating and managing these accounts. During password change cycles, this problem was especially acute, with users frequently forgetting their newly reset passwords.
- It was also necessary to comply with strict data protection laws, such as the DPA or the GDPR. Existing systems were inadequate for monitoring unauthorised access to sensitive patient files, posing a significant risk to patient privacy and organisational compliance.

The outcome

- The IT team chose an identity governance and administration solution to assist in IT operations. The solution changed the game by automating AD account management. The solution's automation capabilities have drastically reduced human error and freed valuable time for their IT staff. This was particularly evident in the streamlined and efficient handling of stale and disabled accounts.
- The solution also empowered users to resolve common issues such as account lockouts independently, significantly reducing service desk calls. This self-service capability has improved user satisfaction and allowed the IT team to focus on more critical tasks.
- The solution also provided a UBA-driven change auditor, which enhanced Bedfordshire Hospitals' security and compliance posture. A crucial aspect of DPA compliance and GDPR compliance is monitoring and reporting unauthorised access to sensitive files. They now have clear insight into their network activities and can protect sensitive patient information.

Cyber Essentials: history and purpose

The NCSC launched Cyber Essentials in 2014 as a UK-based certification scheme. It was designed to provide a minimum level of cybersecurity protection, encouraging organisations to adopt sound information security practices. The scheme quickly gained positive notoriety for its impact on businesses of all sizes. Since October 2014, suppliers to the central UK government handling certain sensitive and personal information must be certified.

The purpose of this program is to help organisations protect themselves against common online threats. This program covers 80% of the most common cyber security threats. There are two levels of certification offered by the scheme: Cyber Essentials and Cyber Essentials Plus. The former involves self-assessment of systems, while the latter requires independent verification by an accredited third party.

In January 2022, the NCSC introduced the most extensive changes to the scheme since its launch. A major factor contributing to this change was the implementation of COVID-19 protocols, digital transformation projects, and a shift to cloud services. The scheme now covers all cloud-based services as well as mobile devices used to access corporate data. Additionally, companies must ensure that all accounts are multi-factor authenticated.

Cyber Essentials is a crucial tool for organisations to protect themselves from cyber threats, demonstrate their commitment to cybersecurity, and win new business.

There are five key controls in Cyber Essentials

These controls provide a baseline level of protection against the most common cyber attacks. Any organisation can implement them, regardless of its size or sector.

Firewall: A firewall acts as a buffer between an IT network and external networks, including the internet. In this way, it keeps private networks from being accessed by unauthorised parties.

Secure configuration: Your servers, computers, and network devices should be configured securely to reduce vulnerabilities.

User access control: A user's access to their account is limited in this control to protect them against misuse and theft.

Malware protection: Malware protection involves preventing your system from being infected with viruses and other harmful software.

Security updates: Make sure your devices and software are up to date. This applies to both operating systems and applications that have been installed.

How Cyber Essentials addresses user lifecycle management

Cyber Essentials certifications provide a foundational set of technical controls that are essential to protecting against cyber threats. Cyber Essentials includes several recommendations regarding managing user access effectively and securely, including key aspects of managing users.

1. **Review process for user creation:** Organisations must have a review process for user creation. This ensures that only authorised users have an account and limits insider threats.
2. **Process for joiners, movers, and leavers:** Establish clear procedures to ensure appropriate access is granted, modified, or revoked quickly for joiners, movers, and leavers.
3. **User account control:** Organisations should ensure user accounts are created with the least privileges necessary. Administrative accounts should only be used for tasks that require administrative privileges. All accounts must be managed to ensure that users have the correct level of access to the systems and data they need for their roles.
4. **Administrative privileges:** Use of privileged accounts should be minimised and controlled. Users should be provided with a separate user account for everyday work, and administrative accounts should only be used when necessary. This reduces the risk of accidental or deliberate misuse of privileged accounts.
5. **Secure authentication:** Organisations should implement strong password policies to ensure all users have robust passwords. This includes password complexity requirements, regular password changes, and multi-factor authentication (MFA) where feasible.
6. **User access control:** Organisations must ensure that access to applications and data is restricted to authorised users only. This involves implementing access control lists (ACLs) and role-based access control (RBAC) to ensure users can only access the information and functionality necessary for their job roles.
7. **Regular review and removal of access rights:** The organisation should regularly review user accounts and permissions to ensure they are still necessary and appropriate for each user's current role within the organisation.
8. **Secure configuration:** Systems should be securely configured to minimise vulnerabilities and reduce unauthorised access. This includes disabling or removing unnecessary user accounts and services.
9. **Monitoring and logging:** Keep logs of significant events, such as user logins and attempts to use privileged accounts. These logs can help identify unauthorised access attempts and be used to investigate security incidents.
10. **Training and awareness:** Training users on cybersecurity importance, including how to choose strong passwords, recognise phishing attempts, and report suspected security incidents.
11. **Incident and response management:** Organisations should have a process in place for responding to suspected security incidents, including how to change passwords and revoke access to compromised accounts.

Healthcare organisations can strengthen their user lifecycle management practices by adhering to these Cyber Essentials controls and recommendations. In addition to minimising insider threats and unauthorised access, this will also improve cybersecurity resilience.

Healthcare organisations can benefit from Cyber Essentials-aligned user lifecycle management practices in several ways:

1. **Increased security:** Cyber Essentials guidelines can help healthcare organisations establish robust authentication mechanisms, access control policies, and user provisioning/deprovisioning processes, enhancing their cybersecurity defences.
2. **Compliance assurance:** The Cyber Essentials certification ensures patient data protection and adherence to best practices in user management, in compliance with regulatory requirements such as GDPR and DPA.
3. **Minimising insider threats:** Using least privilege principles and strict access controls minimises the risks of insider threats and unauthorised access to sensitive patient information, preventing data breaches.
4. **Enhanced operational efficiency:** Efficient user lifecycle management processes reduce IT staff administrative burden and facilitate onboarding and role changes.
5. **Increased trust and reputation:** Demonstrating adherence to Cyber Essentials principles enhances trust and safeguards the reputations of healthcare organisations.

A variety of additional measures can enhance healthcare organisations' cybersecurity posture in the UK after implementing Cyber Essentials. The Cyber Essentials program provides a solid foundation. However, given the sensitive nature of healthcare data and the sector's attractiveness to cyber attackers, additional steps are essential. Healthcare organisations should consider the following advanced cybersecurity measures:

- **End-to-end encryption:** Make sure data is encrypted at rest and in transit. In the case of patient data and other sensitive information, this is especially important.
- **Regular security audits and penetration testing:** Identify and mitigate vulnerabilities by conducting regular security audits and penetration testing.
- **Data loss prevention (DLP) tools:** Incorporate DLP strategies to avoid sensitive information being lost, misused, or accessed by unauthorised users.
- **Compliance with additional standards and frameworks:** Strive for adherence to more rigorous standards, such as ISO 27001 or NIST's Cybersecurity Framework.
- **Secure access for remote users:** Implement secure VPNs, Zero Trust network access, or similar technologies to control remote access to your network.
- **Regular updates and patch management:** Ensure that all systems, software, and devices are updated with the latest patches so that vulnerabilities can be prevented.
- **Network segmentation:** Separate networks to limit user access, prevent malware spread, and protect sensitive data.

- **IoT device security:** Ensure that Internet of Things (IoT) devices are configured, monitored, and isolated from critical networks securely, as these devices are increasingly used in healthcare.
- **Advanced monitoring and detection systems:** Monitor for unusual activity and potential threats in real time using security information and event management (SIEM).
- **Data Security and Protection Toolkit (DSPT):** Complete this online self-assessment, as it is required by the NHS. By doing so, organisations can assess their data security posture and identify areas for improvement. By completing the DSPT annually, you can ensure that best practices and regulations are followed.

In the current environment of constantly evolving cyber threats, it is imperative to review and update cybersecurity strategies on a regular basis.

Emerging trends and technologies are shaping the healthcare cybersecurity landscape, offering innovative solutions to combat evolving cyber threats:

1. **Threat intelligence sharing:** Healthcare organisations are sharing information about cyber threats and vulnerabilities increasingly through threat intelligence sharing initiatives. By collaborating, organisations can proactively identify and respond to emerging threats, enhancing overall cybersecurity resilience.
2. **Artificial intelligence (AI)-driven security analytics:** AI-powered security analytics tools analyse vast amounts of data to identify patterns, anomalies, and potential security breaches in real time. These tools increase the efficiency and accuracy of detecting and mitigating cyber threats through machine learning algorithms and behavioural analytics. Healthcare organizations can strengthen cybersecurity defences more easily when supported by AI.
3. **Zero Trust architecture:** The Zero Trust architecture takes a "never trust, always verify" approach to cybersecurity, requiring continuous authentication and authorisation for all users and devices accessing the network. As a result, this model enhances healthcare network security by minimising the attack surface and preventing attackers from moving laterally within them.

By embracing these emerging trends and technologies, healthcare organisations can adapt to the evolving threat landscape, enhance their cybersecurity posture, and better protect patient data and critical healthcare infrastructure.

Going further, there are several practical steps involved in preparing for the Cyber Essentials certification. These practical tips can help organisations prepare for Cyber Essentials certification and strengthen their cybersecurity capabilities.

1. Analyse your organisation's current cybersecurity posture in relation to Cyber Essentials requirements. Assess any gaps or areas for improvement that need to be addressed to meet the certification requirements.
2. Determine and implement controls needed for Cyber Essentials certification based on gap analysis. Implementing access controls, configuring firewalls, and updating software can be among these steps.

3. Maintain thorough documentation of the steps taken to implement Cyber Essentials controls. As part of this documentation, configuration settings, policy documents, software update evidence, and any other relevant documentation needed to demonstrate certification compliance should be included.
4. Consider engaging with a certified Cyber Essentials practitioner or consultant to assist you with the certification process. They can provide expert advice, gap analysis, and support in implementing the necessary controls.
5. Verify that all controls are working correctly and effectively before undergoing external certification.

The steps to earning a Cyber Essentials certification

The Cyber Essentials certification process involves several steps, as outlined below, and organisations can follow these steps to achieve Cyber Essentials certification and improve cybersecurity resilience.

1. Cyber Essentials certification is open to all UK organizations, regardless of their size or industry. It is especially beneficial to small and medium-sized enterprises (SMEs) looking to improve their cybersecurity posture.
2. Conduct a self-assessment of your organisation's Cyber Essentials compliance. This includes assessing security configurations, firewalls, gateways, access controls, patch management, and malware protection. Cyber Essentials self-assessment questionnaires or certified practitioners can be used to assess your organization's readiness.
3. Engaging with a Cyber Essentials certification body is an option for external certification. Through independent review and testing, these certification bodies assess the organisation's self-assessment and verify compliance with Cyber Essentials requirements.
4. Obtaining a Cyber Essentials certification demonstrates the organisation's commitment to cybersecurity best practices and provides reassurance to customers, partners, and stakeholders.

Safeguarding healthcare cybersecurity's future

Healthcare organisations need a holistic cybersecurity strategy. This includes data encryption, network segmentation, and embracing emerging technologies like threat intelligence and AI-driven security analytics. Organisations must tailor their approach to address their unique challenges and continuously adapt to the evolving threat landscape.

Cyber Essentials certification offers a structured path toward improved cybersecurity posture, compliance, and patient confidence. But it's just the first step. Continuous assessment, adaptation, and collaboration within the healthcare community are crucial for building long-term resilience.

As the healthcare sector navigates the ever-changing cybersecurity landscape, safeguarding the future requires a collective effort from healthcare providers, government bodies, and technology partners. By prioritising cybersecurity, fostering collaboration, and embracing continuous improvement, we can ensure a safe, secure, and trustworthy environment for patient care in the digital age.

Our Products

AD360 | Log360 | ADAudit Plus | ADSelfService Plus
M365 Manager Plus | RecoveryManager Plus

ManageEngine
ADManager Plus

ADManager Plus is an identity governance and administration (IGA) solution that simplifies identity management, ensures security, and improves compliance. With ADManager Plus, manage the user life cycle from provisioning to deprovisioning, run access certification campaigns, orchestrate identity management across enterprise applications, and protect data on your enterprise platforms with regular backups. Use over 200 reports to gain valuable insights into identities and their access rights. Improve the efficiency of your IGA operations with workflows, automations, and role-based access control policies. ADManager Plus' Android and iOS applications help with on-the-go AD and Azure AD management. For more information about ADManager Plus, visit manageengine.com/products/ad-manager/.

$ Get Quote Download