Human Fertilisation & Embryology Authority

Cyber security

Strategic delivery:	☒ Setting standards	☒ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	11		
Paper number	AGC/(13/06/2017) 551		
Meeting date	13 June 2017		
Author	Karl Saunders, System Support Analyst		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to note this report.		
Resource implications	No additional resources, costs incurred within IfQ programme or business as usual expenditure		
Implementation date	Ongoing		
Communication(s)	Ongoing		
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes	None		

1. Introduction and summary

1.1. Cyber security risks have gained a lot of attention in the media due to the recent malware attacks. This has led to a loss of reputation and possible loss of data.

1.2. Malware attacks that recently impacted the NHS trusts have been prevalent for some time. The story behind these malware attacks are very characteristic of any successful cyber-attack, whereby the hackers focus on using known vulnerabilities and then betting on the fact that organisations don't know how to fix what matters.

1.3. This paper sets out to highlight the risks to our organisation, the steps taken to mitigate our exposure to this type of risk and some recommendations with regards to our vulnerabilities. It concludes with a discussion on some 'big' questions we should ask ourselves in the light of the prominence of cyber-threat.

2. Cyber-attack overview

2.1. The recent "WannaCry" cyber-attack is estimated to be the largest attack yet, with more than 300,000 organisations in more than 200 countries falling victim. This attack exploited a known vulnerability in Microsoft windows SMB server, which Microsoft had provided a fix for in March 2017. Unfortunately, many organisations had not applied this fix or were simply running operating systems that had reached their end of life (Windows XP, Windows server 2000) and so no longer received these security fixes. This created the vulnerability for the hackers to exploit.

2.2. The type of malware attack on the NHS is a very general attack so will focus on a known vulnerability. However, no organisation can guarantee the security of its systems against a determined external attacker or internal leaker. Some forms of cyber vulnerabilities can be instigated knowingly or unknowingly from inside the organisation.

2.3. Cyber-attacks are ever changing and can come in many varied forms, with the latest being a focus on hiding a virus within software, it then uses the user's internet browser to steal credentials, download further viruses onto the users' device.

2.4. Another form of cyber-attack can take the form of a compromised web site. This is where a hosted website has been hacked, the hacker will infect a webpage on the site which could either redirect you to another site managed by the hacker and emulate a recognised logon system, enabling the hacker to steal your credentials or tricking you into downloading more viruses.

2.5. A question often asked by those seeking assurance as to vulnerability, is 'I understand the potential for attack, how many attacks have we had, and therefore defended ourselves against?' This is impossible to answer – or at least it would involve disproportionate effort to be able to provide a realistic assessment. Our systems prevent hundreds of emails with attachments and links – some or all potentially injurious – from entering the system in a week. Section 3. Addresses what we do to mitigate the risks, and Section 4. seeks to widen the narrative so that leaders and boards are making effective challenges.

3. HFEA mitigations of cyber risks

3.1. With the introduction of our new desktop estate replacing our Windows 7 machines with the latest Microsoft operating system of Windows 10 we have been able to implement a more robust device management method by deploying Microsoft InTune. This enables us to manage the deployment of fixes from Microsoft to our end users at the earliest opportunity reducing our exposure to these types of risks. InTune also enables us to enforce device policies to mitigate the risks of cyber-attacks. Finally, InTune also enables us to manage the deployment of antivirus software on each end user's device and schedule regular scans of the device.

3.2. In much the same way, we have in place a Microsoft systems management server that manages the patch deployment to our in-house server estate. This is carrying out the patch and virus updates on our 'on premise' infrastructure that InTune is carrying out for out desktop environment.

3.3. The HFEA has a robust backup strategy that that backs up data to two different types of media and we are currently testing a third type of cloud based backup strategy.

3.4. With the deployment of office 365 we have introduced access to cloud storage in the form of OneDrive. This ensures our end users are not saving HFEA data on their local devices, with the possibility of data loss through either a cyber-attack on the individual's device or in the event of a device failure.

3.5. Legacy systems have been either upgraded to more modern operating systems or retired from service and the IFQ programme has also enabled us to deploy parts of our infrastructure into the Azure cloud environment. This cloud approach has significant additional security benefits as part of a managed service.

3.6. Attacks can come in many different forms, infected email, infected removable devices, bundled in with other software and hacked/compromised websites. Some of the greatest weakness in securing a system will be the user interaction with the system. Therefore, it is imperative that all our users know and understand their role in securing both our systems and our reputation. It is paramount that we have a clear and continual message of vigilance with regards to cyber risks. The danger with some of this communication can be that it is often something that is repetitive and can be seen in itself as a form of spam, an irony in itself. The challenge is to keep this information sharing in a relevant and clear way that engages our staff.

4. Questions to ask ourselves

4.1. It is clear that the operational consequences for organisations affected by an attack are potentially enormous. Running alongside this are the reputational risks. Civil Service World, in the light of the recent attack, has set out some useful pointers for public leaders.

4.2. 'It is easy to blame this crisis on some hapless leader who saved money by ending support for XP. But that is like attributing an air crash to 'pilot error', as was normal 30 years ago. Stanley Roscoe, an aviation psychologist of the time, described such conclusions as “the substitution of one mystery for another”. He thought aviation investigators could do much better. They did and so should we.’

4.3. The piece goes on to contrast the civil service being full of intelligent, well-intentioned people, with humans - who are ‘predictably irrational’ and seeing this as both a strength and weakness. We know that people are every organisation’s greatest assets and its greatest risks. It is argued that leaders must understand *behavioural* and *organisational* risks and how to manage them effectively

4.4. ‘Persistently digging to root causes typically reveals an unseen web of human weaknesses that can lie latent, incubating for years – until luck runs out, when they cause a crisis.’ The risk indicators include

- internal silos;
- professionals who saw this coming but were not heard;
- gaps in leadership skill and experience;
- leaders resistant to unwelcome news;
- decision-makers who neither understood IT nor sought explanations;
- inability to learn from history and minor failures;
- incentives that undermine the system’s integrity;
- communication failures;
- cultural weaknesses, complacency and complexity.

These risks are not, of course, limited to cyber-security risks. This paper provides assurance on some of these indicators. In considering our overall appraoch to the management of risk within the HFEA the Committee may have a view on others.

The Executive’s assessment is that we do not display these features, but are alive to each and there is no room for complacency.

5. Recommendation

5.1. The Audit and Governance Committee is asked to:

- Note this report
- Comment on the risk indicators at 4.4