ENSURING THE CYBER SECURITY OF PUBLIC SECTOR ORGANISATIONS

Dan Benn, Lead Journalist, Public Sector Executive

Jim Fox, Cyber Security Specialist, Capita

With the pace of technological change happening every day, organisations need to be prepared to embrace a digital culture. The Covid-19 pandemic brought digital transformation on at lightning speed, with the lockdown forcing organisations to move out of their offices and for many a completely unprepared remote way of working.

With the transition to a more digital way of working, organisations in the public sector had to be even more careful with how they protected themselves from cyber security risks. In order to understand the risks that public sector organisations face and how they can be mitigated, Public Sector Executive recently spoke with Jim Fox – Cyber Security Specialist, Capita, to discuss how organisations combat the issues presented from such a sudden shift in working environments.

Pre-pandemic working conditions were often predicated around an office environment, with very few organisations offering the availability of working from home for prolonged periods of time. As we navigated the Covid-19 virus as a society, we had to adapt these standard working methods to incorporate flexible working protocols which afforded individuals the newfound comfort of operating from their own home office whilst still meeting their workplace objectives. This modal shift of operations has brought comfort and flexibility for employees across the UK; however, it has also presented key challenges for organisations particularly around cyber security.

New issues for a new age

With the introduction of working from home, comes the inevitable widening of gaps as you move into security. When working on-site, organisations were able to make sure that the technology being provided met their requirements and had passed through rigorous checks. Jim believes that this sudden need to adapt to new circumstances left many organisations vulnerable. For example, whilst some organisations provided all of the technology needed - some of them didn't - and as a consequence employees would naturally go to online marketplaces and purchase items of kit to make their office environment easier but use non-approved IT equipment. whilst this may have helped the employee to continue working in the short-term, they inadvertently introduced additional vulnerabilities into the organisation.

Jim also points out that the shift to working from home wasn't strictly the only factor that contributes to weaker cyber security, with the speed of the change playing a significant part. Jim's view is that "organisations pivoted overnight, to change during Covid. With new infrastructure, they've quickly fallen outside their own security requirements and had to introduce policy exceptions at pace. In some cases, these have been numerous and unmanageable", the key point being that they now have unrecognised (and non-compliant) technology solutions.

The general lack of cyber skills is also something that is already causing problems, with organisations employing people that aren't quite as digitally literate as they should be. This means that there is then an even more increased risk of a security breach, due to human error, lack of key skills, or even a more general lack of digital knowledge. If the public sector is to progress even further into the implementation of digital, the lack of skills must be addressed across all sectors, otherwise there is only so much protection that organisations can achieve.

Whilst security is important, Jim also pointed out that there is only so much you can do to keep your network from being compromised there is no silver bullet that guarantees complete security from threat actors. The importance of resilience alongside security ensures that, should an organisation's security be breached, the organisation has the capability and capacity to 'ride out' the issues, to learn lessons quickly, implement them and ensure that similar issues cannot happen again, Jim says "dealing with an incident should be part of a continual cycle."

Ensuring resilience

With the threat of having your network compromised, also comes the inevitable threat to the data that you hold. Public sector organisations hold a vast amount of data in various forms and locations, this ranges from personal data of people in a constituency, financial information, or crucial information about the day to day running of the organisation.

Losing any of this data is a significant challenge for any organisation irrespective of size, the brand impact, potential for regulatory punishment and possible civil litigation is significant however there are ways of ensuring that you mitigate these. Jim emphasised that preparations should begin even before a critical event happens. He said that "it's only unexpected when the organisation hasn't foreseen the incident and had adequate plans in place for it. Almost all common cyber incidents can be foreseen and should have plans in place, this includes how you respond, how to resolve and how you recover. Resilient organisations need appropriate and agile business continuity plans, including cyber response and recovery plans, IT disaster recovery plans and a wider crisis management plan for your senior leadership team. You have to mitigate and remediate the problem; this includes also dealing with the impact, understanding the problem, resolving the issues, and patching the vulnerability that has allowed the hacker to come into your network, all with the usual IT staff resource level whilst also maintaining a day-to-day service for your customers."

The pace of development of new technology is a leading factor as to why organisations need to be more aware of the risks that they face, there also needs to be some element of keeping informed on new emerging technologies that may surface in the future. The future of technology is constantly developing and evolving, to the point where it is important that everyone has sufficient horizon scanning capabilities, certainly those who are in charge of the digital aspects of running an organisation, is aware of what technology could be just around the corner.

Looking to the future

Technology is constantly evolving, and organisations will always be behind the curve. The advent of quantum computing, the internet of things (IoT), and artificial intelligence has the potential to be game-changers for organisations, however if they are implemented incorrectly or deployed in the wrong environment, without critical supporting packages, then this could create more problems than they were intended to solve, such as loss of data or network outages.

If we take artificial intelligence, for example, it can do the work of many staff members and could be more cost effective with the ability to work continually throughout the day and night. It is also able to complete lower value tasks, freeing up employees to focus on other more high value objectives. However, because it is technology, it will still need human oversight, not to mention compliance with ethical, moral, and legal requirements and obligations. For example, at what point do you decide that AI cannot be used for certain decisions.

Taking the next step

Organisations need to complete a review of their technology estate, as it stands today, understanding what they have, what is connected, where it is located, and who has access to them. Their corporate policies should be reviewed and approved at governance level in order to ensure that the new estate has been fully approved and meets corporate requirements.

Having an effective threat intelligence capability, such as monitoring social media or commissioning a third party to provide updates on their behalf, is something that organisations should be considering. This should also be backed up by a triage process, as well as clear options, should anything of concern be discovered.

If organisations in the public sector are to ensure that they are safe from cyber incidents, there is a lot to do. This does not mean, however, that once a security system has been established, the organisations can rest on their laurels. Yes, they should have an effective response plan to all known cyber incident types, and they should be tested at least annually, however it is also crucial to ensure that organisations have a mechanism that allows to keep up to date with emerging technologies, understanding their benefits and risks, as well as ensuring that they have invested in keeping up with the ever-changing skills requirements. If the lack of skills is addressed, and the skills progress as the technology does, then organisations may just stand a good chance at ensuring not only security, but also resilience against cyber threats. The most common scenarios that cause the most impact are data-breach, ransomware, and network outage scenarios.

Jim Fox, Cyber Security Specialist, Capita

Capita's Managed security services

Our managed security services capability provides industry-leading cyber security design, implementation, monitoring, management, threat intelligence and incident response expertise. Our dedicated security operations centres provide comprehensive cyber expertise to protect organisations, staff, customers and citizens.

Get in touch

Find out more