and human behaviour, thus providing a clearer picture to make improvements. Are devices accurately encrypted? Is the same security clearance given across all IT systems? How can visibility of the devices used by employees improve? These are just a few areas where an audit can provide clarity to an organisation.

BYOD seems a natural solution for SMEs to gain the mobility and accessibility they require to successfully compete. But to truly gain the full potential from BYOD, organisations must understand the security threat that comes with it. This understanding must run through the entire hierarchy of an organisation and combating it must be seen as a collective effort rather than being left to the IT team to deal with. Solutions such as COPE and MDM all serve to improve the clarity of the devices used and address the security challenges with these.

Placing BYOD as an SME business priority will also need to be equally matched by cyber-security enforcement; considering cyber-security as an afterthought will only lead to further complications for SMEs down the line.

About the author

Kevin Timms is the COO and co-founder of IT services aggregator, Streamwire. Prior to this, he had over 35 years' experience in the automotive industry as an IT director for both Ford and Jaguar Land Rover, where he held roles in both Europe and the US. Timms graduated from Queen Mary University, having studied material science. He is trustee director of the British Motor Museum.

References

1. 'Data breaches increase 40% in 2016, finds new report from Identity Theft Resource Centre and CyberScout'. Identity Theft Resource Centre, 19 Jan 2017. Accessed Jun 2017. www.idtheftcentre.org/2016databreaches.html.
2. 'BYOD and Mobile Security'. Crowd Research Partners, 2016. Accessed Jun 2017. http://crowdresearchpartners.com/wp-content/uploads/2016/03/BYOD-and-Mobile-Security-Report-2016.pdf.
3. 'Mobile Security: Guarding the Enterprise'. Enterprise Mobility Exchange. Accessed June 2017. www.enterprisemobilityexchange.com/eme-security/white-papers/mobile-security-guarding-the-enterprise.
4. 'Global Cyber-security Assurance Report Card'. Tenable. Accessed Jun 2017. www.tenable.com/lp/2017-global-cyber-security-assurance-report-card/.

Cyber-security in government: reducing the risk

Joe Kim

Joe Kim, SolarWinds

In May of last year, the UK Government reported that two-thirds of the country's large businesses had been hit by a cyber-attack within the previous 12 months.[1] Therefore it's no surprise that cyber-security is high on the agenda for the Government – highlighted by the recent £1.9bn investment into a five-year cyber-security strategy that was set into motion in February 2017 with the official opening of the National Cyber Security Centre.[2,3]

A data breach or cyber-attack can cost government organisations thousands or even millions of pounds to rectify. But it's not just the loss of money that is of concern. The damage to reputation and the impact on citizens' privacy caused by a breach of highly sensitive personal data can be devastating.

Syphoning sensitive health information, in particular, is an increasingly lucrative pursuit. Health credentials can be sold for $10 a pop on the black market, which is 10 to 20 times the value a cyber-criminal can get for a credit card number.[4]

Late last year, around 1,000 patients came very close to having their procedures cancelled at three UK hospitals managed by the North Lincolnshire and Goole trust.[5] A computer virus infected critical systems and resulted in officials declaring a "major incident". In this instance, the breach could have had a very serious impact on patient health and wellbeing.

So, what does this mean for individual government IT teams? Cyber-security needs to be baked into every corner of every government organisation. From finance administration to front-line workers, everyone needs to play a part in keeping government infrastructure safe and secure. So let's look at some steps that government IT teams can take to help protect their organisations from determined cyber-criminals looking for a lucrative payday.

Educating the end-user

Ultimately, you could say that the security of the network comes down to the IT team rather than the end user. However, even the savviest cyber-security team will struggle to protect an organisation if employees aren't aware of security threats. Ensuring that employees are educated in the basics of cyber-security is crucial.

With bring your own device (BYOD) increasing in popularity, end-user education is more important than ever. BYOD is now commonly perceived as an expectation rather than a perk. Employees must be educated in the potential risk that their personal device presents to the entire network and their responsibility as an employee to minimise the risk of a cyber-attack infiltrating the network from their personal device.

Educating end-users doesn't need to be overly complex – keep it simple and put a clear plan in place. Start with an awareness programme that encompasses education and enforcement. Demonstrate the serious implications and potential devastation that can be caused when hackers infiltrate the network and encourage all employees to be 'vigilant protectors'.

Monitoring and alerts

Monitoring the network and setting up alerts to swiftly identify suspicious activity is critical. With sophisticated device monitoring, a malicious insider shouldn't be able to access and save sensitive data onto an external device. Systems should be in place to immediately identify foreign devices and eject or automatically block suspicious activity. All government organisations should have a solution in place that offers sophisticated monitoring and alerts.

On top of alerts, which notify the IT professional after a problem has occurred, it's also possible to instantly detect suspicious network activity or requests from unknown sources using real-time data. When an attack takes place, data-driven analysis can provide root-cause analysis to help the IT team better understand how the attack happened and how far it has spread, as well as helping to mitigate a similar instance in the future.

Risk management decision-making

It's easy to get caught up in the hype and fear surrounding cyber-security and to want to protect every corner of the business from a potential breach. Unfortunately, this isn't always possible and the IT professional needs to prioritise. We know that is often easier said than done.

One way to decide where limited budgets and resources should be spent is through a risk assessment. Once upon a time, professional risk managers were commonplace in organisations. They would assess technical equipment, systems and software and assign the monetary value of the risk if an individual piece of equipment was hit by a virus and/or went down. This once old-fashioned approach should make a comeback in the face of cybercrime, not only to educate the rest of the business on the importance of cyber-security, but also to provide important guidance on optimising investment and minimising organisational risk.

The National Cyber Security Centre is part of a five-year strategy by the UK Government, costing £1.9bn.

Up-to-date technology

Keeping security technology and tools updated is a critical and simple – yet often overlooked – method of maintaining a secure network. Using outdated device firmware, insecure protocols and outdated security technology can leave the organisation wide open to attackers. For example, telnet is still regularly used on organisational networks, which is tremendously outdated and can be vulnerable to cyber-attacks.

This doesn't necessarily mean digging into precious budget and forking out for brand new kit. Instead, it could simply mean installing the latest updates when prompted, rather than wishing you had, following an attack. Undertaking a simple audit to ascertain which technologies require an update can be a very effective exercise to help minimise organisational risk.