

## **Network Box white paper: Securing the Public Sector**

### **A Network Box guide to IT Security in the Public Sector**

Recent years have seen a number of high-profile security breaches hit the public sector. Data privacy in particular is a serious concern, and is more tightly governed than ever before, with higher penalties for organisations that don't comply effectively with legislation. At the same time, more public service business is conducted online, as information is distributed to citizens through web-based applications.

This guide addresses some of the key security issues facing the public sector; and gives practical advice on security measures to take in order to avoid breaches that can carry high costs to an organisation, both financially and in reputation terms.

#### **Key issues facing the public sector**

##### **Most security breaches are caused by human error**

Human error covers a multitude of sins: from an employee falling victim to a phishing attack; to leaving a laptop on a train with unencrypted data on it. Good security management can significantly reduce the risk of human error causing a breach. But this doesn't just apply to the end user, but also to the IT department. You can have the best security systems in the world in place, but if you don't keep them updated, or misconfigure the firewall, or change an application without checking the impact that has on security, then your systems may be rendered useless.

In 2009, a number of hospitals fell victim to Conficker, many months after patches were made by the manufacturer that would have made those very systems immune to the infection. If security had been updated correctly, the breaches could have been avoided.

##### **We all do more online**

From filing tax returns, to paying rent, to ordering prescriptions – more public services are available online than ever before. This creates a web-facing layer to the IT systems of public sector organisations, a move away from the closed environments of the past. With this increase in web-based applications across the public sector comes an increased risk of security breaches – from criminals accessing personal information, to launching SQL injection attacks.

## Data has a value to cyber-criminals

Organisations keep more data, and for longer, than ever before. From patient records to electorate information, this data is valuable to cyber-criminals, and any organisation that holds data is a potential target for a hacker. Whether it's stealing an identity, launching a phishing campaign, or cloning credit card information, consumer data has intrinsic value to cyber-criminals, so must be kept secure.

## Public sector budgets are under pressure

All public sector spending is under review, and this isn't likely to change in the next three years. Although security is one area of IT unlikely to be cut from budgets entirely, the pressure is on to: reduce or halt capital outlay; reduce management time and resource; and reduce total cost of ownership.

## More employees work from home, at least some of the time

Flexible or home working can seem to be a security headache. But with proper planning and the provision of secure access via Virtual Private Networks (VPNs), organisations can create secure home working environments for employees.

## We all interact more online

We see some serious vulnerabilities in 'social' or rogue applications that are creeping into businesses as they are downloaded by employees, (such as P2P software – see our guidelines on this here: <http://www.network-box.co.uk/sites/default/files/nb-guide-to-p2p-security.pdf>). These are often inherently insecure, as they are not built with business purposes in mind.

## How to address these issues: best practice considerations for public sector organisations

1. *Make human error harder.* Make sure you have the most up-to-date security systems and patches in place; and that you regularly check for the latest versions of applications or platforms used across the organisation – including your security applications: firewall, IDP, VPN and anti-malware - as they may include critical security updates. For more information, see our [guide to updating systems](#).
2. *Remember that security is about more than just email.* In 2009, we saw a clear move by cyber-criminals towards focusing on exploiting vulnerabilities in applications, web browsers and servers, rather than just mailing executable code. As a result, you should integrate anti-spam, anti-virus and firewall to other critical protection, including intrusion detection and prevention (IDP), application security, VPN, and content filtering.
3. Review what applications and systems are used across the organisation as part of your ISO9001 meetings or about once per quarter. The security team must work to ensure they are aware of vulnerabilities in all systems from Internet facing routers to new web applications. Set clear user access rights and guidelines to ensure that all users understand what they should and shouldn't be using. For more information, see our [guide to monitoring applications](#).

4. *Ensure that all data is routed through the appropriate channels and that nothing bypasses security systems* (this is one of the most common causes of vulnerabilities). For more information, see our [guide to routing](#).
5. *Educate employees*. Hold security training at least once a year for each employee, to review security procedures and to make sure that all employees understand their role in keeping an organisation secure. Limit access rights so that only employees who really need access to certain applications or platforms have it.
6. *Use a secure VPN for home workers*. With more of us working from home at least some of the time, the risks of a security breach increase (for example, if the computer used is also used by other family members). Consider issuing a work computer to regular home workers that is configured to the organisation's security standards. Data carried between work and home on memory sticks or mobile devices can get lost in transit. Far better to allow access only via a secure VPN. See our [guide to remote working](#) for more information.
7. *Don't allow employees to download anything that isn't approved by the security team* – particularly P2P software or platforms, that can open up a clear route through the organisation's security. Even commonly-used platforms such as IM must be checked to ensure that it is routed via the right secure channels and updated regularly, to avoid leaving a 'back door' open to a hacker.
8. *Encrypt any data that has to be moved*, and ensure mobile devices and laptops are securely password protected. Where possible, use multi-factor authentication (our [guide to authentication](#) for more information).
9. *Check all data leaving the building*, in the same way that you check data that comes in (via any communication channel, such as IM or email). This will help prevent unauthorised transfer of data that could lead to compromised security.
10. *Tap into expert knowledge* by bringing in specialist security experts to run your security systems. Getting an external, approved managed service company can [reduce costs by between 20 and 40 per cent](#), with no capital outlay.

**For more information on securing your company network, visit**  
<http://www.network-box.co.uk>, or  
call James Mackie on 0800 107 6098

**To keep up with news from Network Box, see Simon Heron's blog:**  
<http://blog.network-box.co.uk>; or follow him on Twitter:  
<http://www.twitter.com/networkbox>.