

Network Box white paper: A guide to IT security for hotels

In 2009, the Radisson hotel group revealed that it had been the [subject of a server hack](#) that compromised the personal details (including credit cards) of guests for six months. In January this year, [V3](#) reported that the international hotel group Wyndham Hotels announced that it too had been the [subject of a hack](#), with data and credit card details stolen.

It threw into sharp relief the issue of data privacy for hotels. Aside from credit card details, hotels may often hold personal information about guests including their home addresses, frequent traveller schemes, date of birth, passport information and so on.

As more reservations and financial transactions are done online, and guest data is stored by the hotels on central servers, privacy is becoming more of a critical issue. Data security is demanded not just by the public, but by law. And yet often the IT security systems of hotels have holes in them.

This guide is designed to help the IT managers of hotels to understand the security risks, and to provide practical advice on tightening up security measures to minimise the risk of breaches that can carry high costs to an organisation, both financially and in reputation terms.

Key IT security issues facing hotels

Who has access to your systems?

John Walker, of the Information Systems Security Association points out in [an article for Computing magazine](#) that the IT systems of hotels are often on display. He cites a number of examples of lax security, such as that of a hotel whose staff directed him to leave his baggage in an unlocked room that gave him access not just to the hotel's IT systems, but also to its user manuals, that were stored on a shelf in the room.

Equally, an unmanned computer could offer up guest data to a professional criminal, or an opportunist (from inside or outside the hotel) to steal valuable data. Time out systems and secure passwords should be used for all databases.

Sadly, these scenarios and others like them are not uncommon, and put the security of hotels and their guests at serious risk.

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 reception staff leaving a computer unattended with a guest's details on the screen. Good security management can significantly reduce the risk

of human error causing a breach. Train staff on the importance of IT security; ensure they stick to security guidelines; and make sure that you have the most up to date protection in place.

Data should be treated as securely as a guest's personal belongings

The increase in the number of online reservations and interactions between a guest and the hotel means an inevitable increase in the risk of security breaches. In the same way that you wouldn't leave a guest's hotel room door open for passers-by to wander in, so their personal data should be protected and kept secure. Locking the door on data means ensuring that all IT systems, applications, and platforms that 'touch' the data are properly managed, and secured by firewall, anti-virus, intrusion detection and prevention, and remote access is secured by VPNs (if data is stored centrally, for example the headquarters of a hotel chain).

Data has a value to cyber-criminals

Any organisation that holds data on customers is a potential target for a hacker. Hotel guest data might include the kind of personal details that could allow a hacker access to bank account (date of birth, account details, clues to passwords etc) and will have a clear value to criminals. 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.

Hotel budgets are under pressure

IT spending for hotels is notoriously kept under pressure. But the financial (and reputational) cost to a hotel of a data breach could far outweigh that of a good security system. Budgets are tight, and IT systems must be proven to reduce management time and resource; and reduce total cost of ownership.

Flexibility to secure different levels of Internet access for employees and guests

Security systems must be flexible enough to deal with both employee internet access and guest access. One Network Box customer, [Wyboston Lakes](#) - which includes a hotel, serviced offices and conference centre - has to provide security that is flexible enough to meet individual requirements for each of its serviced office clients, as well as guests and delegates. It has to ensure the highest possible level of security in terms of spam, viruses and other malware, but needs flexible internet access and VPN policies to suit different needs. For example, Wyboston restricts what websites employees can access (such as adult sites and social networks) and applications such as IM, but allows more freedom to hotel visitors.

How to address these issues: best practice considerations for hotels

1. *Limit access to your IT systems.* Do not share server room space (particularly not with luggage!) and keep your servers behind securely locked doors.
2. *Use time out systems* to ensure unused systems become inaccessible.
3. Limit the number of employees who can access personal guest data (and then only with the use of strong passwords). For more information on passwords, see our [advice on password security](#).

4. *Make human error harder.* Educate employees on the importance of tight security systems, and their role in keeping guests' data secure. Hold security training at least once a year for hotel employees, to review security procedures and to make sure that all employees understand their role in keeping an organisation secure.
5. *Ensure all security systems are kept up to date;* 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](#).
6. *Encrypt guest data.* No sensitive data should be left unencrypted; and personal guest information should never be sent over an unsecured system (such as email).
7. *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](#).
8. *Set internet access rights.* Hotel guests can have more flexibility than employees, so ring fence their internet access so they can't download malware onto the hotel network. Block access to blacklisted websites altogether.
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 guests' 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>.