A guide to cyber security risks for Hospitality and Hotels

THE CYBER RESILIENCE CENTRE FOR THE SOUTH EAST

Privacy

As well as data breaches and loss of data, another important aspect is the privacy rights of your customers. Do you have an accurate privacy statement publicly available on your website and on your hotel guest registration cards that clearly spells out why you are collecting their private information and how you intend to process that data? The guest must opt-in to you processing their data.

Of course, some collecting and processing is a necessity, such as reserving a hotel room, and the guest would have to opt-in as part of the reservation, but what about other activities such as marketing and post reservation contact? It must be clear to the guest if they are opting in to receive marketing contact via email, phone or mail, and they must be able to choose to opt-out at any time. Failure to abide by a guest's preferences can receive equal attention and possible fines from the ICO.

The Confidentiality, Integrity and Availability Approach (CIA)

- Once you have a reservation in your systems, you now have to protect the data. Your Information Security Program should consider the CIA approach. In Cybersecurity, CIA refers to protecting the Confidentiality, Integrity and Availability of your data.
- Confidentiality is about keeping the data secret and only allowing authorised access to it.
- Integrity is the assurance that the information is trustworthy and accurate.
- Availability is a guarantee of reliable access to the data by authorised people

Confidentiality

- To maintain confidentially, use the Role Based Access (RBAC) principle. For example, if you collect credit card data as part of your reservation process, do your reception staff need access to that info to perform their role, or should that level of access be reserved for your finance team?

- As well as authorised access from internal staff, a big risk here is unauthorised access to your systems from a cybersecurity attack. If you are primarily using a wifi network for your systems access, make sure you have implemented a strong wifi password using WPA2 encryption, and change the default password on your router. If you have a more sophisticated network with switch equipment, ensure you keep these up to date with the latest firmware.
-
- Up to date firmware is also important for your router and wireless access points. Much like computer operating systems, constant new vulnerabilities are being discovered that must be patched against to reduce risks. Consider your computers and servers in use at your business. Protection measures have matured considerably since traditional anti-virus software which relied on a file of virus signatures to be regularly downloaded and used to detect a virus. End Point Detection and Response systems can now be used in tandem with anti-virus to conduct real-time analysis and detection of threats for a much more proactive approach.

Passwords

Passwords are just one of the layers of defence to systems security but are easily bypassed if they are simple words, easily guessable, shared between staff, never changed or even worse, written down by the computer. Ensure you and your staff are following password best practice:

- Use complex passwords, using combinations of letters, numbers, symbols and the longer the better
- Change the password regularly
- Do not use the same password across multiple systems or applications
- Do not share passwords
- Do not write passwords down

Integrity

To protect Integrity and ensure data has not been tampered with, a number of security controls can be employed, and many overlap with protecting confidentiality. Data should be encrypted in databases and other storage medium and encrypted in transit along with digital certificates. An email sent with a digital signature proves that the email was sent from the originator and the receiver cannot deny receipt.

Availability & Ransomware

Availability might just be the hot topic now, with incidents involving Ransomware attacks growing at an exponential rate. With Ransomware, a hacker encrypts your files and data on a compromised system and, literally, holds them to ransom. You are asked to pay a ransom amount, usually in bitcoin, so it remains untraceable, and then your files are released. Monetising attacks in this manner is proving more profitable, and therefore more popular than selling stolen data.

However, sometimes this is combined, and this is also the threat you are given if you refuse to pay. What kind of disruption would happen in your business if your Hotel booking system or Property Management System was made unavailable in this manner? Imagine the queue at the front desk at check-in time!! To combat ransomware, we have to look at it from two angles, reducing the risk of it happening in the first place, and being able to recover if it does, without paying.

Phishing

The most common way for ransomware, and actually most system compromises, is Phishing, where you or a member of your team are tricked into clicking on a link or opening an attachment in an email that looks genuine to you. The link will either lead you to a fake website where you may key in login info or credit card information, or the link may download malicious software to your computer for further compromise activity, such as encrypting your data and initiating a ransomware attack. This is the same for the attachment, which will likely contain malicious code to run on your computer.

Falling for a phishing email is relatively easy. Think about the emails you receive daily running a hotel. An enquiry for a group booking with an attachment of names, a guest querying details of a reservation with their reservation details attached, the delivery of an item to the hotel with a link to the delivery details.

Teach your staff to spot these tell tale warning signs:

- Email is not addressed to you in person
- A sense of urgency is requested
- The email address behind the “name” of the email sender does not match
- Does the domain name of the sender’s address match the organisation supposedly sending the email
- The URL of any links are not in context with the message or the organization’s domain
- Misspellings either in email addresses or generally in the body of the email
- Poorly written with bad grammar

Physical security of payment terminals

On a more physical security note, an area that is often overlooked, but is a PCI requirement, is the safety and security of your credit card payment terminals. Restaurants and bars are often unsupervised when not open, which means your payment terminals could be at risk of tampering or substitution. The criminal aims here to collect credit card data which may be transmitted via wifi to a remote device. The best practice is to lock away the terminals when the F&B area is closed but there is still a risk of tampering when the area is open, so you need to inspect your terminals to look for signs of tampering regularly.

Things to look for would be overlays on the keypad, a broken security seal which is normally stuck across the join of the front and back of the device, an additional cable that wasn't there before, or perhaps scratches where the device has been opened. To make this easy, you can take pictures of the device, but if you regularly inspect you should have a good understanding of what is normal. To the letter of PCI, you need to keep an inventory of your terminals, along with key information such as the serial number.

Even if the terminal is not tampered with, it has been known for criminals to work in pairs, distract the bar staff and steal the device from behind the bar. They could then carry out a refund to a credit card before returning the terminal behind the bar, unnoticed. So keep terminals out of reach at the back of the bar if possible. As a business that takes credit cards for payment you are obligated to your acquiring bank to be PCI compliant so you should familiarise yourself with the full set of PCI requirements.

Use of public computers

So our guest has booked their stay, arrived at the hotel, has used the bar and other facilities. They now need to print a ticket to take to a show they have booked for their stay, so they use the PC and printer you have made available in the reception or business area specifically for guest use. This poses more security risks as we need to ensure personal information from the previous use of the PC is not left behind. The easiest way to achieve this is to use a managed kiosk software package that automatically cleanses the PC of all data after each use. If you don't use this type of software, you would need to manually clear caches, web history, print queues and any files created.

Another check that should be performed regularly is to make sure a rogue USB device has not been connected, unseen, at the back of the PC. This could be running any kind of malware, but likely is a key logger that could capture all info entered by guests, such as logins and passwords to online banking or credit cards for a purchase. The criminal would simply return after a time and retrieve the USB device.

Breach notification

Should things not go to plan and a breach occurs, you must know your obligations to the regulatory bodies to report the breach and any notifications you must make to guests whose data has been lost or stolen. You can find out the requirements at the Information Commissioner's Office website: https://ico.org.uk/for-organisations/report-a-breach/

Where you have external partners and suppliers that may handle guest data on your behalf, you must ensure they are contractually obliged to protect the data. With the inception of the EU GPDR law and now UK Data Protection Act, you are directly responsible for this and cannot just shift liability to your suppliers.

Quick Checklist

THE CYBER RESILIENCE CENTRE FOR THE SOUTH EAST

Now that you have read through the cyber security risks that hotels can face, please use our simple checklist to ensure you are mitigating against any risks that might present themselves.

- [ ] Have an accurate Privacy Statement in place, accessible to guests and customers
- [ ] Scan and test your website for common vulnerabilities
- [ ] Use Role Based Access for systems and applications access
- [ ] Update firmware on network equipment
- [ ] Change default passwords on network equipment
- [ ] Apply operating system patches to PCs and Servers
- [ ] Keep applications up to date with current releases
- [ ] Use a modern anti-virus and endpoint detection system on your computers
- [ ] Use complex passwords and change them regularly
- [ ] Encrypt sensitive data when stored and in transmission
- [ ] Regularly check your payment terminals for tampering or substitution
- [ ] Keep your payment terminals physically safe
- [ ] Ensure guest data is cleansed from PCs made available to guests after use
- [ ] Inspect guest use PCs for rogue USB devices
- [ ] Familiarise yourself with breach notification requirements
- [ ] Inventory and categorise data, and apply the right controls to each level
- [ ] Securely delete or destroy data when it no longer has a business use
- [ ] Train your staff on phishing attacks and how to spot them
- [ ] Contact the South East Cyber Resilience Centre to see how we can help you