cardonet
making IT happen

Protecting Hotels from Cyber Attack

Part of the Revenue and Reputation series of whitepapers and reports for hotels by Cardonet.

Cardonet IT Support & Solutions
7 Stean Street London E8 4ED
0203 024 2244 | www.cardonet.co.uk | info@cardonet.co.uk

Contents

1. Introduction

In April 2017, the UK-based Intercontinental Hotel Group (IHG) disclosed that 1,200 of its franchise properties were struck by payment card stealing malware. An investigation detected malware in front-of-desk payment systems between 29 September and 29 December 2016, no doubt to surreptitiously collect customers' bank details. Guests have been advised to closely monitor their bank statements
.
There are a few interesting take-aways from the case:

1. Following the discovery, IHG offered its franchised properties a free examination by an external computer forensic team but a number of its hotel managers have declined to take-up the offer

2. Franchise hotels with encryption-based security measures haven't been hit

The first revelation shows that some hotels still under-estimate the extent of their exposure (and the ramifications of falling victim to a cyber-attack).

The second demonstrates that taking a proactive approach to security really does make a difference. In general, criminals will pursue the quick wins.

Cyber criminals are also quite strategic in their methods. While every kind and size of company should take cyber security seriously, there are certain industries and types of businesses that are more prone to attack than others.

A few years ago, the retail sector suffered a series of high profile security breaches, forcing the industry to shore-up its defences. As retail companies have become harder to penetrate, cyber criminals have shifted their gaze to the next easy target - the hotel sector.

Hotels are now coming under attack from several different fronts. Most of which will lead to financial loss for the hotel, some will directly target their guests and damage the hotel's reputation. All will distract the hotel from delivering on its prime calling – to provide an excellent customer experience.

When you consider the great lengths hotels go to, to source the right furnishings, beauty treatments, breakfast buffet, fitness equipment and so on, their failure to sufficiently secure their systems and protect their guests from identity theft, makes all the other luxuries quickly pale in significance.

This paper will aim to furnish hotels with the information they need to protect themselves from opportunistic individuals, intent on enriching themselves at the expense of others, while causing as much mischief as possible. While the threat is huge, hotels only need to take simple measures to resolve their security flaws, starting with educating their staff.

> As recent PWC figures show half of UK companies expect to be attacked within the next two years, the spectre of falling victim to a cyber-attack is no doubt keeping hoteliers awake at night. But the cost, trouble and embarrassment of suffering a breach doesn't have to be a foregone conclusion. Simple steps can be taken to prevent such an attack at best, or minimise the fall-out at worst.
>
> Sagi D. Saltoun
> Cardonet Managing Director

Attacks that hurt the hotel's bank balance

1. Ransomware: ruthlessly and efficiently extorts money from hotels

2. Phishing scams: fool hotel staff into handing over access to company online bank accounts

Attacks that target the hotel and damage its good name in the process

1. Denial of Service: cause hotel websites to grind to a standstill, inconveniencing would-be guests - resulting in loss of earnings

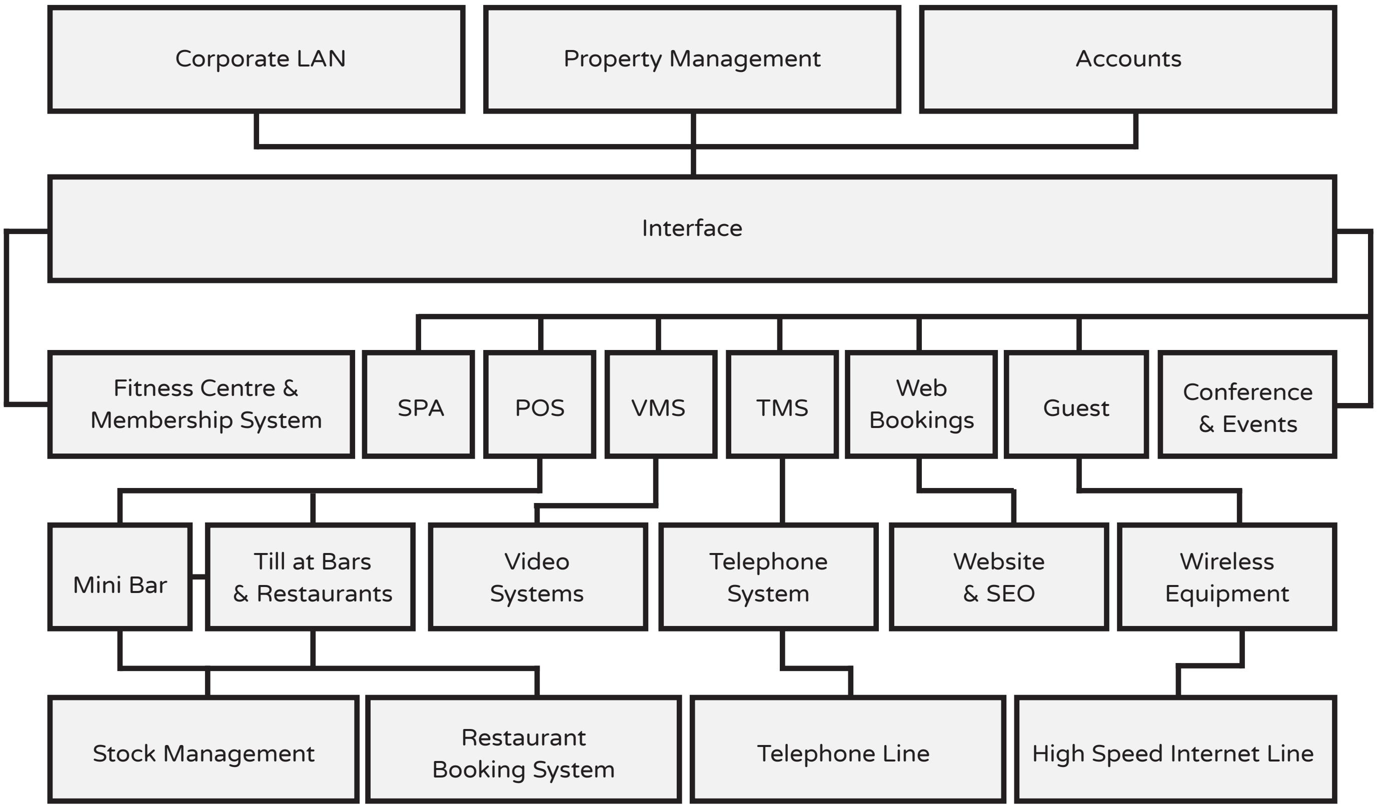
2. Malware: steal guests' credit card information from unsecured POS or other hotel IT systems

2. Rich pickings

Hotels are hospitable – to their patrons and any cyber criminal that wants to ransack their computer systems. Given the wide array of disparate systems in any one hotel and the high net wealth of their clientele, hotels represent rich pickings.

The visual below shows an average hotel network and the many potential entry points for a creative intruder. They might devise a strategy to access the system from the Corporate LAN or Property Management suite of tools - or via the bar and restaurant tills. Although the Point of Sale system still remains the most popular avenue, for many this is pick n mix heaven.

A typical hotel network



3. The changing threat landscape

The Romans won battles because they had a strategy. While most military commanders of the day simply ordered their troops to rush wildly at the enemy, the Romans kept their men in order, adjusted their formations and took their enemies by surprise. Through these means, they created an empire that at its height, stretched from north-western Europe to the Near East and encompassed all the lands of the Mediterranean. They set the bar for modern warfare, which is now so intelligent, it can be deftly controlled from behind computer screens.

Similarly, cyber criminals have a broad arsenal of techniques at their disposal, to force entry into a hotel system or dupe staff into opening the gates to them.

a) Malware

In 2015 five major hotel groups: Hilton Worldwide, The Trump Hotel Collection, Starwood, Mandarin Oriental, and White Lodging Properties confirmed data breaches nationally and internationally (as IHG has done so recently). Each hack involved malware, malicious code that infected point of sale systems at gift shops, restaurants, bars and other on-property technology, to expose the identities and credit or debit card information of guests paying for these services.

However, cyber criminals don’t just target large organisations. Small businesses, including boutique hotels, are also popular targets. In 2015, 74% of SMEs suffered a data breach (up by 14% from 2014) – many of which would have been caused by malware.

Malware is stealthy. For months, it can intrude upon a hotel system and steal sensitive information like customers’ credit card details, undetected. Once news gets out, a hotel’s reputation can be left in tatters – not to mention its bookings.

b) Ransomware

Just as common infections and viruses develop a resistance to medicine over time, cyber criminals are evolving their techniques. Ransomware, a pernicious type of malware, is the latest ‘attack of choice’.

It prevents or limits users’ ability to access their system, either by locking their screen or placing certain files hostage (data kidnapping). Cybercriminals then force users to pay a ransom through anonymous online payment methods to access a decrypt/unlock key.

The whole situation is costly and stressful, particularly as paying the ransom doesn’t always mean the criminals will keep their end of the bargain and share the decryption key to recover the hotel’s data.

It’s a terrifying notion but without a comprehensive data-back-up, a company would be powerless to defend itself. If a criminal, with no scruples, says jump, all they can do is say ‘how high’, with no fore-knowledge of when the jumping will end.

All of this cost, heartache and hassle comes from just opening an attachment from spammed email, unwittingly downloading malicious pages or running unpatched systems, vulnerable to exploit kits and malware.

c) Denial-of-Service attacks

The integration of ‘smart’ devices into our homes, businesses and hotels is both an opportunity and a risk. On the one hand, the Internet of Things (IoT) is yielding unprecedented opportunities to delight your guests, unearth greater efficiencies and make cost savings through automation. On the other, IoT devices are giving cyber criminals many more entry points for attack.

According to BH Consulting, a lot of these devices are rushed to market, without fully baked-in security features; an opinion that is shared by many IT professionals. Three quarters of 7,000 IT professionals polled think IoT device manufacturers are not implementing sufficient security measures on their devices.

And then there’s the issue of access. Many of these devices still use widely known default passwords. Meaning anyone that hasn’t changed the passwords on their devices is enabling such attacks. Because many of these devices are managed on the same network (via a hotel WiFi which is normally kept open), it’s relatively easy to manipulate a device in one room, from another.

These weaknesses ‘invite’ criminals to wreak major disruption through insecure IoT technology. This was on show for all to see in October 2016, when IT savvy criminals targeted hundreds of thousands of unsecured internet connected digital devices, such as home routers and surveillance cameras, smart lighting and even door entry systems, to launch crippling Distributed Denial-of-Service (DDoS) attacks using the Mirai botnet management framework.

One of their strategic targets was DNS service provider Dyn. By toppling Dyn, the first domino in a long line, a trail of sites collapsed. Airbnb was one of these. It experienced service outages and along with many other affected brands, learnt first-hand, the implications of an insecure networked environment.

d) Phishing

Phishing remains the world’s most popular and effective attack vector. Phishing is the fraudulent practice of pretending to be something you are not and inducing individuals to reveal personal information, such as passwords and credit card numbers. Spear-phishing, which is highly customised, often lulls users into a false sense of security by including personal information in a correspondence – information a user might assume only the people they know, services they use and brands they buy from, would know. In actual fact, this information is ‘harvested’ from social networking sites, or stolen.

When it comes to the hotel sector, a common way to launch an attack is to fool someone into downloading a malicious script, sent via email, targeted at hotel staff. However, cyber criminals are continually reviewing their techniques. For instance, they recently contaminated a credit card authorisation Word document used by a small luxury hotel chain, to install a particularly resilient strand of malware on any machine that opens it. Because of the custom nature of the malware, the hotel’s antivirus software didn’t catch it, suggesting the criminals had conducted reconnaissance work, to obtain the document and circumvent the firewall.

Sobering global statistics

- Volume of unique malware samples: 60m in 2016
- Total malware attack attempts: 7.87bn
- Ransomware incidences: 638m (167x increase on 2015)
- By the end of the first quarter of 2016, $209m in ransom was paid by companies
- Companies in the UK were almost three times as likely to be targeted with ransom ware as companies in the US

Source: SonicWall Annual Threat Report 2017

> The threat landscape appears to have evolved and shifted. Cyber security is not a battle of attrition; it’s an arms race, and both sides are proving exceptionally innovative.
>
> Sonicwall Annual Threat Report 2017

4. Defence strategy

Despite the changing threat landscape, one thing remains constant: most cybercriminals, like house burglars, look for easy hits. If a hotel's network is secure, they'll move onto the next target. The key point is to stay vigilant - it only takes one corrupted email attachment to wreak havoc on an organisation.

This is a clarion call for hotels that run their operations on unsecured networks. Fortunately, these systems can be patched and fortified with the right know-how. However, staff also have to be educated about the human component of cyber security - the fact that criminals will bet on staff error time and time again.

> Every case involving cybercrime that I've been involved in, I've never found a master criminal sitting somewhere in Russia or Hong Kong or Beijing. It always ends up that somebody at the company did something they weren't supposed to do. They read an email, went to a website they weren't supposed to.
>
> Frank Abagnale
> American security consultant and the subject of the Academy Award-nominated feature film Catch Me If You Can.

Part of this education starts with understanding the range of threats levelled at an organisation at any one time. If a hotel has any hope of preventing its very own cybergedden, it needs to understand its vulnerabilities, which means never taking anything for granted and testing everything, including its own kit, which will have its own entry points. It also means asking important questions. For instance, how long would it take for a guest to connect their laptop to the corporate network before anyone notices? By posing the right questions, a hotel can build an effective cyber-security strategy.

In May 2016, the UK government exhorted companies to beef-up their cyber security capabilities. Its Cyber Security Breaches Survey revealed that while one in four large firms experience a data breach at least once a month, only half of all firms have taken any recommended actions to identify and address these vulnerabilities.

The Minister for the digital economy at the time noted that too many firms are haemorrhaging money, data and consumer confidence through a lack of action.

What should a hotel's defence strategy entail?

1. Technical control
2. Administrative control
3. Compliance

a) Technical control

Know your vulnerabilities

- Use a spam filter to safely quarantine suspected spam, viruses and phishing emails
- Test your systems for uninspected backdoors
- Monitor and patch vulnerabilities (always test the patches before applying them)
- Segregate at-risk computers or software from critical data and services

Check the locks

- Install next-generation firewalls and plan for regular updates
- Use cable locks to prevent the unauthorised removal of ethernet cables, patch cords, IP phone cables, and other components from sensitive ports that could destabilize network connections
- Control and monitor access to your comms room
- Use lock screen time outs for PCs, laptops and other devices
- Place publicly accessible systems on isolated networks

Back-up and securely store your data

- Keep at least two copies of your data; in addition to the original location you should have an on-site and a secure off-site back up
- Maintain a constant, automated backup schedule
- Encrypt your backups with good tools and strong passwords, and keep those passwords safe.

b) Administrative control

You should have company-wide security policies and standards in place, instituting change controls (e.g. access to machines or email addresses) and configuration controls, and do background checks of contractors and employees.

Educate your employees and encourage a best-practice environment whereby, log out of terminals after they've finished their work and report suspicious behaviour. Help employees to discern between phishing emails and genuine communications by sharing the common tell-tale signs:

- Mismatched url
- Misleading domain name (people who launch phishing scams often depend on their victims not knowing how the DNS naming structure for domains works)
- Poor grammar and spelling
- Slightly doctored or inferior company logo or email template
- Requests for personal information (a formal company wouldn't use email for such a correspondence)
- An email alerting you to a billing anomaly that asks you to click for further information

c) Compliance

Compliance includes all of the above. To comply with stringent data protection standards like PCI DSS companies must show they have taken the necessary steps to gain technical control and administrative control.

Meet PCI DSS requirements

As you're no doubt aware, all entities that process, store or transmit cardholder data must comply with the Payment Card Industry Data Security Standard (PCI DSS)
In the event of a security breach, a compromised entity such as a hotel, that is not PCI compliant is subject to additional card scheme penalties, such as fines. This isn't too problematic except that the PCI Compliance checklist is very long (comprising more than 600+ items), and while you might think compliance will safeguard your organisation in perpetuity, former PCI Standards Council General Manager Bob Russo once indicated that liabilities could change depending on the state of a given organisation when an actual breach occurs – meaning continually striving for best practice is paramount.

Ironically, although PoS systems are particularly vulnerable to infiltration, hotel credit card machines aren't always PCI compliant. Hotels often try to reduce security hurdles upfront, to ease the customer experience in the short-term, without considering the possible ramifications of lowering the barriers of entry for an attack.

In response to the question above – "what should companies do?" – the answer is to go above and beyond and demonstrate due diligence in all areas (as a hotel would when it comes to matters of health and safety).

This involves investing in the right expertise – whether that expertise is in-house or through an IT company that prides itself on filling the space between a resident IT team and an outsourced managed IT service.

Your IT team must take it upon themselves to "know" the network, the business processes and data flows. And then of course they should be able to follow recommended actions, for instance segmenting cardholder data and restricting access to USB ports.

Cracking PCI DSS won't only protect a hotel from attack, it will also mitigate any damage done, if it is attacked.

Be GDPR ready

In early 2018, the much-discussed General Data Protection Regulations (GDPR) will come into force. Media reports and our own intelligence suggests that hotels aren't ready. From 28th March, if a hotel suffers a data breach, not only will they have to pay criminals (if hotel computers have been corrupted with ransomware), PCI DSS fines, higher insurance premiums, clean-up costs; while weathering the financial blow of losing good faith in their brand, they'll also have to pay the Information Commissioner's (ICO) penalties. Under GDPR, companies can be fined up to €20m or 4% of annual worldwide turnover, whichever is greater. These figures will far exceed the current maximum fine of £500,000 issued by the ICO – representing a double whammy for the victim of the cyber-attack – the hotel (while the criminal gets off scot-free and quite a bit richer).

All of this means the clock is ticking. Hotels have a finite amount of time to secure a wide and disparate network of systems, while fending off attacks from increasingly inventive and sophisticated cyber criminals.

5. Find sanctuary from the storm

When you consider the level and intensity of attacks aimed at the hotel sector, the cocktail of penalties that a hotel will face from falling victim to an attack and the reputational damage that it will incur – it's clear that the hotel industry is facing a perfect storm.

This inclement weather comes at a time when hotels are facing stiff competition from the likes of Airbnb, flipkey (another holiday rental and room sharing site), tripping (a growing search engine for lettings), as well as ranking sites like TripAdvisor, which are putting hotels through their paces.

Cardonet has been providing IT support, expert IT project delivery and strategic IT services to the hotel and hospitality industry since 1999. It helps hotels manage their disparate and business-critical systems, by bringing its extensive knowledge of industry-specific solutions to the table (including Opera, Brilliant, Guestline, Micros, Ving, VDA and more), to ensure they're deployed in the most effective, secure and resilient way possible.

With Cardonet IT Support & Solutions, you are in safe hands.

Glossary

Cybergedden - a state of emergency resulting from a large-scale sabotage of all computer networks.

DOS - a denial-of-service attack typically floods servers, systems or networks with traffic in order to overwhelm and incapacitate the victim’s resources/website.

DNS - Domain Name System - the Internet’s system for converting alphabetic names into numeric IP addresses.

GDPR - The General Data Protection Regulation is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union.

Hacking- an unauthorized intrusion into a computer or a network. The perpetrators (hackers) may alter the system or its security features for their own ends.

Internet of Things - the interconnection of computing devices embedded in everyday objects, enabling them to send and receive data.

LAN – a local area network is a network that connects computers and other devices in a relatively small area, typically a single building or a group of buildings.

Malware - software which is specifically designed to disrupt, damage or gain authorised access to a computer system.

PCI DSS - Payment Card Industry Data Security Standard. A proprietary information security standard for organisations that handle branded credit cards from the major card schemes.

Phishing - the fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information

Ransomware - a type of malicious software designed to block access to a computer system until a sum of money is paid.

Spear-phishing - an email-spoofing attack that targets a specific organisation or individual, to elicit sensitive information. It’s targeted rather than random.

WAN - A wide area network is a geographically distributed private telecommunications network that interconnects multiple local area networks (LANs). May consist of connections to a company’s headquarters, branch offices etc.

This whitepaper on cyber security is part of the revenue and reputation series of whitepapers and reports for hotels by Cardonet.

EXPERTS IN IT SUPPORT & SOLUTIONS FOR HOTELS
Cardonet has been providing outsourced IT support, expert IT project delivery and strategic IT services to the hotel and hospitality industry since 1999.

We know that:

- You need an IT partner who can build an IT roadmap that keeps you ahead of the competition and provide director-level business intelligence.

- Your team need 24x7x365 proactive support and systems that “just work” so they can concentrate your guests.

- Your guests need super-fast Wi-Fi and technology that works around-the-clock.

Cardonet is the only IT team your business will ever need to build the infrastructure, support the systems and advise you on the projects that will maintain your competitive advantage.

cardonet
making IT happen

Cardonet IT Support & Solutions
7 Stean Street London, E8 4ED
T 0203 024 2244
E info@cardonet.co.uk
www.cardonet.co.uk