GYM OWNER monthly

Website:www.gymownermonthly.co.uk
Date: 16.11.17

BUSINESS

Time to take action on data security risks

Paul Simpson, Chief Operating Officer, at *Legend Club Management Systems* explains why it is now imperative that leisure operators take action on data use and protection as a top business priority.

There is now rarely a week goes by without a new data security breach story hitting the press. Awareness has certainly risen in the light of recent events, specifically since the global WannaCry ransomware attack which crippled parts of the NHS, and our own industry specific PayAsUGym attack in December 2016.

Unfortunately, increased awareness of data security has so far not equated to action. Indeed, there is the continued threat that ignorance of basic information security principles and obligations is placing the leisure industry at significant risk. Given the volume and extent of personal and financial information routinely collected by leisure operators, our industry is not only a soft target but a particularly vulnerable one. Without adequate precautions to minimise the risk of data breaches, operators leave themselves vulnerable to threats which could extend far beyond regulatory fines and brand damage: it could permanently undermine trust and lead to business failure.

GYM OWNER monthly

Website:www.gymownermonthly.co.uk
Date: 16.11.17

BUSINESS

Inherent data vulnerability

The information an organisation holds is arguably its most important asset. In the leisure industry, the quantum of personal data routinely collected has grown in magnitude and leisure operators are custodians of a volume of detailed information on members - both young and old.

With the growing recognition that data is today's currency, leisure businesses are increasingly vulnerable to a range of data security threats, from accidental misadventure to financial fraud and other criminal intents. Data breaches can occur in many forms and include stealing passwords, malware attacks, back door application vulnerabilities, insider threats, permission excesses, physical attacks and the biggest threat of all - user error.

Common user error breaches include the obvious - incorrect handling of credit card data - and the less obvious, such as paper based member health and fitness information stored in unlocked filing cabinets. Routine tasks undertaken daily by front of house staff are often conducted without essential data safeguards in place. Often, too little staff education is provided as to essential data security protocols and their importance.

As an issue, information security is complicated by the specific challenges of the leisure industry. Rapid turnover of staff makes it difficult to consistently apply information security training to all staff handling customer data. The result is inadequate information security on the ground that jeopardises both personal safety and business longevity.

Unfortunately, as an unregulated industry there has historically been little to no guidance provided regarding the safeguarding of information. While existing legislation, including the Data Protection Act (DPA), and the Payment Card Industry Data Security Standards (PCI DSS) require very specific data security processes and policies, many in the leisure industry would be hard pressed to demonstrate compliance with them.

Business implications

The impact of a system that is breached holds wide ranging implications and liabilities for companies, ranging from hefty financial penalties through to commercially damaging systems down time, reputational and brand damage.

The impending arrival of the EU General Data Protection Regulation (GDPR) in May 2018, further muddies the playing field. The higher penalties and specific requirements regarding information security, as well as the need to inform any individual affected by a data breach within 72 hours, demand the attention of any business owner and / or operator.

The UK Payment Card Industry Security Standards Council (PCI SSC) has warned that UK businesses could face up to £122bn in penalties for data breaches when GDPR comes into effect in 2018. It has also stated that regulatory fines would be dwarfed by the reputational damage incurred by a data breach. Reputational damage, business disruption and revenue loss await those who deal with this topic lightly. Moreover, if customers lose confidence in an establishment's ability to safeguard personal data, then the online portals and payment processes which have streamlined our

GYM OWNER monthly

Website:www.gymownermonthly.co.uk
Date: 16.11.17

Creating a new ethos: Confidentiality, Availability & Integrity

It is clear: information security can no longer be an issue peripheral to main business functions. It is now a vital legal requirement that companies adopt as part of everyday operations. Moreover, security best practice is not about a reaction to external events. It is not a one off process, nor a sudden decision to update virus protection or patch vulnerabilities. On the contrary: security requires a pro-active culture and a security minded ethos at all levels. It demands continuous attention and the emphasis must be on securing information - not just technology systems.

To safeguard valuable information, organisations need to think about their information assets first. What information does the business hold? Where is it located? Is it up to date? Is it still required? Is it digital - or are paper records still in use? Are employees accessing information via their own devices? By considering every piece of information in line with the three guiding principles of security - confidentiality, availability and integrity - organisations can begin to understand how to protect their data assets.

Confidentiality is assurance of data privacy, achieved by ensuring data is only accessed by authorised individuals - this requires excellent access controls for information systems and ensuring good internal processes for the use of paper based documentation. Availability demands that data is available when it is needed - a ransomware attack, for example, denies this. Integrity is about ensuring data is accurate and up to date.

There are two specific areas of the GDPR where focus will need to be applied by leisure operators. One of these is 'consent', which places robust criteria on the positive obtaining of consent from the individual for the processing of personal data. The second is that of data retention and the individual's 'right to be forgotten'. These two areas will need careful assessment to ensure there is a clear business need for data to be held for specific time periods and consent is held to do so. Some data retention needs will be legislative (such as tax records) and others business (such as usage). The current lack of a clear retention policy amongst many operators will need to be addressed.

Time to take action

In light of the current environment no organisation can afford not to completely rethink their approach to information security. Despite the lack of clear security guidelines in the health and fitness industry, GDPR casts a clear spotlight on our legal and moral duty to take a proactive approach to protect and secure customer data. This is a real opportunity for businesses to embrace the new regulation; to expand our current view of information beyond that held electronically to include all information assets in the business, and embed best practice within our daily operations that includes a physical infrastructure and an ethical security culture, that will protect both business and customer data, for the long term.

Responsible for Legend's ISO27001 Information Security Accreditation, Paul Simpson Legend's Chief Operating Officer is happy to make his expertise available to those who have industry GDPR/ information security concerns.

Paul can be contacted on gdpr@legendware.co.uk or visit www.legendware.co.uk/accreditations.