Multi-unit operations, of course, often use the Internet as the two-way link back to the corporate office, usually for access to the local systems data and to download new menu items and pricing. Corporate Intranets are also invaluable for quick and flexible access to operations manuals, discussion forums, company news items, a corporate documents library, e-mail between sites and many other purposes.

Given enough bandwidth, chains can also use on-site video cameras to check on operations remotely and to help train staff by monitoring their actions. Careful use is obviously required with this! It's great to keep an eye on how busy a restaurant is, or to pinpoint a new server who's having trouble with some basic functions and provide specific training, but if the staff feel that they are being spied on all kinds of issues can arise. Owners should absolutely be able to monitor cash registers and managers' offices (with their safes) from a remote site. Surveillance system recorders should definitely be located away from the restaurant. Many a restaurant has been robbed and intelligent thieves have walked out with the video systems that recorded the theft because they were located in the very spot that was being robbed.

Wireless Internet access in casual dining environments is nearly ubiquitous; so much so that its presence may not draw customers in, but its absence will certainly keep them away. Providing customers with free internet access can be disadvantageous as it greatly increases the incidence of "camping," so think carefully before offering such a service.

SECURITY

No mention of information systems would be complete without a discussion of security. Security has been left for last, but it is one of the most important considerations in any information system management plan. Protecting the security of a restaurant's information is of paramount importance. A recent study at the University of Nevada Las Vegas found that hoteliers consistently overestimated the adequacy of their IS security systems. One of the reasons for the lack of appreciation of security may be that there is little apparent ROI for investments in information systems security. Systems security measures mitigate risk and there is no real way to quantify risk, but the cost of a systems security breach can be catastrophic.

The risk associated with a breach of information systems security is very high. No sector of the business community is exempt from attacks on their information systems. Many thousands of these attacks occur on a routine daily basis and result in extreme financial losses. These attacks have taken on a myriad of forms, including computer-assisted fraud, spying, vandalism, and hacking. Many of these attacks involve attempts by thieves to gain access to customer credit card data, and these attempts constitute a major portion of the risk inherent in IS security.

© 2009—American Hotel & Lodging Association. All rights reserved.

In order to address these concerns major credit card companies created an organization—the Payment Card Industry Security Standards Council[1](commonly known as PCI)—to ensure that any business accepting credit cards adhered to a strict set of standards for IS security. Failure to adhere to these standards is very risky for business, in terms of liability for fines, card replacement costs and most importantly, loss of customer goodwill. The overwhelming majority of restaurants in operation today are not PCI compliant.

The PCI standards require that all merchants build and maintain a secure network, take steps to encrypt and protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test their networks, and maintain an information security policy. Measuring a restaurant's compliance with PCI standards is also a useful measure of how well the business is guarding data other than credit card information. The same six standards should be adhered to when assessing the security of proprietary data, as the damage that could be done to a business by a breach of its other IS systems is potentially as great as if credit card data are compromised. In other words, a breach could cost you your business.

Wireless networks, in particular, are extremely vulnerable. To protect them requires more than the simple use of passwords, virus scans, or a firewall if any sensitive data are being transmitted via the network. The best systems for protecting wireless data transmissions are those that utilize a strong form of the extensible authentication protocol (EAP). EAP supports a number of different authentication schemes and can fulfill the relevant requirements for PCI compliance.

CONCLUSION

F&B management isn't going to get any simpler or easier. It's always going to rely on creative people to set the atmosphere, and on people-focused managers to provide excellent guest service and to keep a motivated, guest-focused staff happy and productive, in a world with slim margins and traditionally high employee turnover.

The industry has reached the point where the use of information systems is a neceesity, and that these systems must be integrated to provide management with the tools necessary to compete effectively in a drastically constricted economy. The slim profit margins by which restaurants normally operate have become razor thin. It is absolutely essential that information systems be utilized effectively to create as much value as possible. Like all the best tools, they become intuitive and invisible to their most practiced users, and creative managers will take full advantage of them to maximize both guest satisfaction and profits.

1 See the AH&LA publication "The PCI Compliance Planning Process for Lodging Establishments"

© 2009—American Hotel & Lodging Association. All rights reserved.