Securing Your IT Assets – The Time Is Now

by Phil LaBelle & Amitava Chatterjee, CHTP

Information technology (IT) assets are an integral part of a hotel's business portfolio. This includes traditional wired networks connecting hotel employees with centralized application services, corporate Intranet, e-mail systems and the Internet. For many hotels it also includes wireless networks, providing guests with high-speed Internet access (HSIA) in meeting rooms, guestrooms and common areas, and providing employees with an un-tethered alternative to the traditional wired network. How safe are these systems and networks?

Some of the potential high risk areas for your IT assets are discussed here as well as suggestions to ensure and promote a safe and secure environment for a hotel's guests and employees. This discussion should lead the reader to spend a few moments thinking about the security of their own environment.

Risks

It is crucial for hotels to understand the risks faced by their IT assets and to have a risk mitigation and/or risk response strategy in place. Potential security issues range from inappropriate access to theft of guests' personal or financial data (and the resulting liability issues), to malicious denial-of-service attacks on a hotel's computer systems. Hotels must assess risks against external and internal factors that contribute to IT asset security (or the lack thereof). External factors are outside our control and internal factors are within our control. Hacker intrusions and network attacks, viruses, worms and spamming are some of the external factors. Untested and inadequate disaster recovery plans, loose data storage and system restore policies, insecure wireless infrastructure and careless employee discipline are some of the internal factors.

External Factors

In his paper on disaster recovery, Tedd Gordon writes that external attacks "can pose greater risks to information technology (IT) operations than hurricanes, floods, power outages and the like[1]." The distributed nature of today's computing environment allows many opportunities for potential wrongdoers to cause havoc.

Hackers, Worms and Viruses

Hackers seek out vulnerabilities by using computers to find weaknesses and backdoor entryways into corporate networks. Once inside they can plant viruses and worms capable of seeking out addresses in address books and mass-mailing spam messages to them, stealing sensitive guest and employee data and information of a competitive advantage nature. Their efforts may be thwarted by incorporating secure hardware and software firewalls. The network must be monitored against unwelcome intrusions, and must be capable of shutting out external threats. But before you get too comfortable, consider this. While hackers outside the company get most of the press, it's a statistical fact that most security breaches originate on the inside.

Internal Factors

Disaster Recovery Plans

This is a good time to check whether or not your own internal disaster recovery plans (DRP) are sufficient. Hotels must ensure that their DRPs are regularly tested and that frontline employees know their roles and responsibilities in the event of a network failure. These should be discussed as a part of their daily pre-shift briefing. When was the last time your hotel ran its no computer system reports? These reports would be invaluable in the event of an IT outage and would generally include a list of in-house guests, an expected arrivals report for the next few days and an open balances report.

Data Backups

Data backups are important safeguards toward information security. Hotels must follow a robust backup methodology. Backup media must be clearly labeled and stored offsite in a secure location. They must only be accessible to authenticated, authorized individuals. It is not enough to merely have a backup storage and retrieval process in place. Periodic tests must be conducted to verify that the resulting backups actually fulfill their intended purpose (i.e., restoring a complete working system). If your hotel's technology infrastructure is hosted in a data center, visit the facilities and familiarize yourself with their data

backup methodology. Are they taking the necessary precautions to safeguard your data?

Wireless Network Security

Many hotels now provide wireless connectivity facilities for their guests. Unsecured wireless networks are dangerous. Smart hackers can use packet sniffing tools and detect what is going on within your computer networks—your data will be at risk if security controls are missing. Adequate care must be taken to ensure the security of wireless networks. This can be done by employing some kind of encryption and network access controls to prevent unauthorized use.

Corporate Leaders Must Take Responsibility

A task force of several companies working alongside the U.S. government has issued a set of guidelines encouraging corporate leaders to take responsibility for network security. The recommendations issued on April 12, 2004 by the corporate governance task force of the National Cyber Security Partnership trace guidelines previously established. The task force set forth a security governance framework, identified network-assessment tools and recommended that companies adopting the guidelines should formally state their intentions on their Web sites.

The task force also recommended that companies should conduct periodic risk assessments, assign explicit individual roles in security management structures and use best-practices guidance such as the ISO 17799 to measure their security performance. It also recommended CEOs conduct annual security evaluations.[2]

Compliance Management

With a plethora of security compliance guidelines and bulletins, such as urgent notices from software vendors to install patches to protect against software vulnerabilities, it is important to ensure that the appropriate compliance monitoring mechanisms are in place. Compliance monitoring will go a long way in safeguarding the security of your IT assets. Who is responsible in your organization? Who is monitoring compliance? Who is verifying that everything is working as it should? According to Michael Rasmussen, Forrester Research[3], successful compliance management involves:

- **accountability** — understanding that executive management and the board are ultimately accountable for compliance;
- **governance** — establishing a culture of compliance in the organization;
- **responsibility** — appointing someone to be in charge of compliance management;
- **understanding** — identifying what the regulators are looking for;
- **architecture** — developing a compliance control architecture; and
- **validation** — verification that controls are in place and functioning properly.

Hotels should be aware of the external and internal factors that place their IT infrastructure at risk. Robust risk mitigation and risk response strategies must be in place and regularly tested. Hotels must monitor security compliance and ensure that adequate controls are in place—all these efforts will go a long way in safeguarding your IT assets.

Phil LaBelle (philip.e.labelle@us.ibm.com) is an IT architect with IBM's Travel and Transportation, Hospitality & Leisure industry, where Amitava Chatterjee, CHTP (amitava.chatterjee@us.ibm.com) is an advanced consultant.

Sources

1 Gordon, Tedd, Vice President, IBM Global Services, Business Continuity and Recovery Services. Disaster Recovery Planning. Toigo, J.W. 2000 Prentice Hall.

2 Task force issues network security guidelines. Carlson, C. http://www.eweek.com, April 12, 2004.

3 Demystifying Compliance. Rasmussen, M. Forrester Research, March 2004.