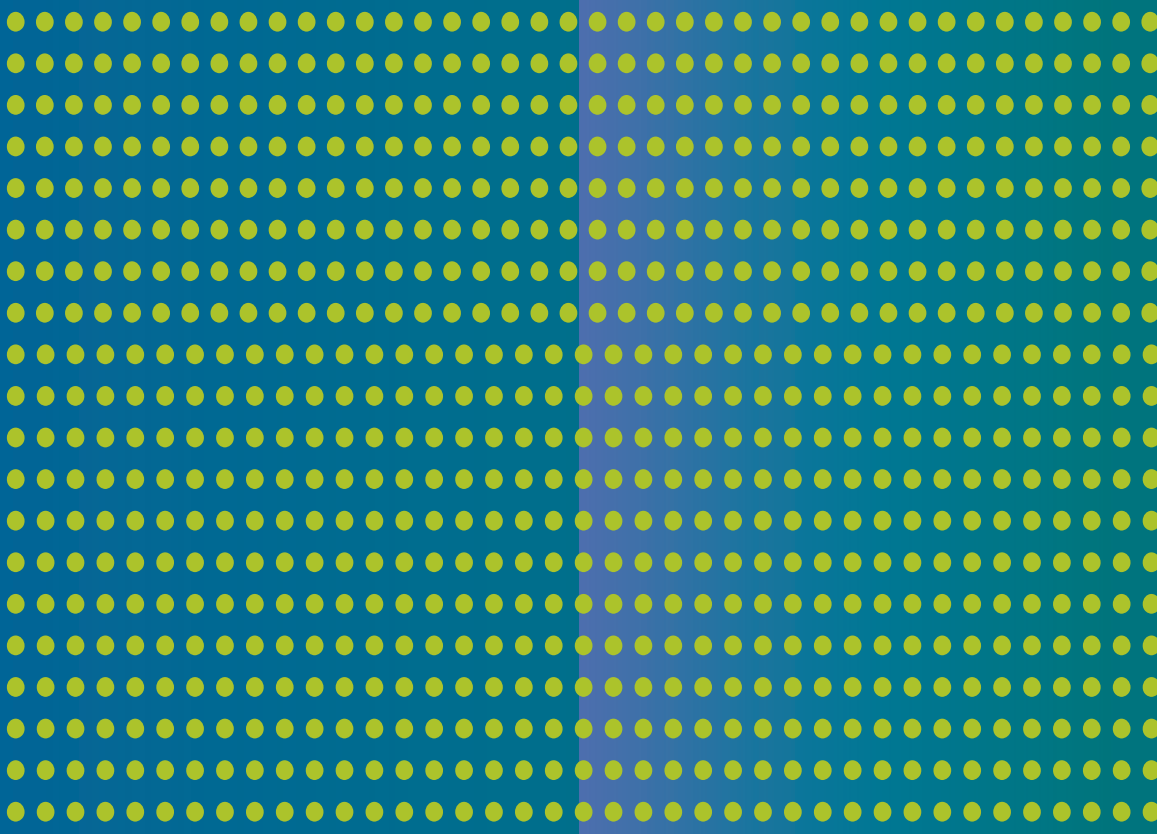
PEARSON NEW INTERNATIONAL EDITION

Technology Strategies for the Hospitality Industry

Peter Nyheim Daniel Connolly

Second Edition



ALWAYS LEARNING™

PEARSON®

Pearson New International Edition

Technology Strategies
for the Hospitality Industry
Peter Nyheim Daniel Connolly
Second Edition

PEARSON®

(voice, IM, fax, etc.) can be managed in one mailbox which facilitates communication in our fast-moving industry.

11. SECURITY

Security issues are a great concern when using networks and the Internet. Virtualization, as one example, can open up your network to malicious software spreading much faster than older networks. Meeting this need, newer classes of networks using Internet technology have sprung up, providing businesses with a secure way of conducting transactions in such a public environment. Currently, ISPs and organizations utilize **virtual private networks (VPNs)**. A VPN provides a secure connection to different sites of an enterprise over the Internet. Specific protocols are used that wrap data transfer, inhibiting penetration from unauthorized users. With innovations such as this, secure transmissions are further enabled. Now companies can offer telecommuting options to their workers. This allows off-site workers comparable access to the same data and network speeds while at home or away from the office. VPN's effectiveness has led to it also becoming a standard for internal or company networks.

The degree of access, if at all, given to others using a network calls for difficult decisions. Granting and restricting access to Internet resources is done by software known as a firewall. **Firewalls** prohibit unauthorized users from accessing Internet resources through user verification and passwords. Advanced firewalls also monitor Internet intrusions and attacks. A popular form of attack is a *denial of service attack* where routers and other devices on the Internet are co-opted and form what is known as a **botnet** and are directed to a specific Web site. The volume overwhelms a Web server and prohibits other users from accessing its resources, rendering it useless. Botnets may also spread viruses, **worms**, **Trojan horses**, and **spyware**. Viruses are malicious pieces of software; worms, Trojan horses, and spyware work a little differently. While a virus needs an end-user to activate it (unknowingly), say opening an attachment which ends in .exe (Don't do it!), a worm does not. Worms exploit information on your computer (e.g., e-mail addresses) and spread themselves without human interaction. Trojan horses are phony software that appear to do one thing but once installed do another, such as deleting files, whereas spyware can record passwords and key strokes. Be careful what you install and click online!

Due to the Internet's designed public nature, oftentimes the Web server is put out in front and separated from other network resources. The area between the Web server and the rest of the network is given a military-sounding name, the demilitarized zone (DMZ). Use of firewalls and placement of servers often dictate how remote workers can and cannot access company resources such as files and e-mails.

Firewalls play an important role in network protection. Good network administrators will update their firewalls daily against the malicious pieces of software. Smaller hospitality organizations with network connections provided by DSL or cable modems do not realize that their connection is continuous, making their computer more vulnerable to malicious software. To prevent this, firewalls must be used. It is often surprising to organizations that use advanced firewalls with monitoring capabilities how often an attempted or successful intrusion happens on their network. Larger organizations can see thousands of attempts daily, yes daily.

Communication between different networks has its own security issues, particularly when the Internet is used for such privileged data as credit card numbers. In addition to the methods used by VPNs, scrambling of messages, known as **encryption**, is often necessary to keep transmissions

private. Encryption involves a mathematical operation that assigns different values to a key. Given the discussion of 8 bits representing a specific key, encryption assigns more 1s and 0s algorithmically to each key to mask the actual keys used, and thereby the entire message. The number of additional 1s and 0s used represents the strength of the encryption method used. Common cost-effective encryption methods used today are 128 bits. Luckily, there comes a point where it is cost-prohibitive to attempt to crack higher encryption methods. It simply takes too much processing power and time. Unfortunately, technological advances in encryption are also taking place in the nefarious encryption cracking software realm.

Security issues are more local than one might think. Studies show that most breaches or thefts of company data are done internally. A locked door and restricted access can solve many problems. On the other hand, external threats are often at a lower level than you may think. They are enabled by telephone tricks where one party calls another and tricks that party into giving access information. This is an example of **social engineering**. Oftentimes, hackers, or those who penetrate a network, use social engineering methods to get in the door of a network and wreak havoc on Web sites or illegally obtain data. For these reasons, network administrators concern themselves daily with a host of issues. The first issue deals with user authentication. Currently, user identifications and passwords are commonly used. Other tools include rights and permissions of data. For example, a housekeeper is not given access to sales data, nor is a member of the wait staff given client home phone numbers. By restricting who has access, many problems can be avoided. Having proper policies in place can also aid in network security. Letting employees know about current phishing e-mails is a common one. **Phishing** is broadly defined as fake e-mails that trick the user into providing information such as social security or bank account numbers. In the age of employee empowerment, data access must be studied constantly by all levels of management. Advanced network software development has created **network behavior analysis (NBA)** software which analyzes a network for irregularities.

Advanced identification technology such as iris (eye) and fingerprint scanning along with facial recognition take away many of the vulnerabilities of password and user IDs. Costs have dropped to a degree that fingerprint technology is becoming more common as a password replacement.

While smart phones have enabled much more personalized access by both management and the guest, security must be applied here as well. Proprietary corporate property may reside on many smart phones, so passwords at a minimum are needed. Aside from the aforementioned content regarding security, smart phone security software is available, giving the administrator many options on what can be done with both the corporate phone and guest access.

12. Summary

Network understanding is now a required tool for any hospitality manager. We use it daily and so do our guests. From small networks, found in a restaurant, to larger global hotel communication systems, network knowledge is a must. When a network goes down or is not used properly, lost revenue and unhappy customers can result. Executives meet this challenge by first applying the right combination of network topography, mediums, transmission technologies, and smart phone integration into their organization. With the proper foundation in place, network offerings such as wireless access, IP TV, and VOIP can be used to their fullest potential. Other networks, such as telephone, electronic data interchange, wireless systems, and cloud computing are equally important, and can be used to benefit the organization and guest alike. Growing in importance

by the day is network security. Up-to-date firewall software and data encryption are a good start, particularly when considering that customers' personal information and credit card numbers make up much of the network data. A true security strategy including employee policy and procedures, which is tested often, serves as a true complement to any hardware or software. No matter what organization you are in, networks require constant attention.

13. Case Study and Learning Activity

Case Study

Julie is the assistant general manager for a local independent hotel. She was recently hired due to her technological expertise. The owners of the hotel wished to increase their property's network security. Other hotels in the area were the victims of security breaches, and the owners feared that they would be next.

Julie knew from her training and past experience that what needed first was a situational analysis to find points of vulnerability. She wanted to handle the major problem spots first before she dug into the more technical matters and relatively quickly identified some potential hazards. She compiled a list of the first ten vulnerable points she encountered and turned it over to the owners that morning.

Vulnerabilities

1. Front desk staff is giving out too much information over the telephone
2. The room holding the network servers is unlocked
3. The computer system does not require users to change their passwords often enough
4. Both guests and employees use the same network
5. Employee and guest cell phones can access the hotel's wireless network
6. Firewall software requires manual updates
7. No employee network policy currently exists
8. Software installation is allowed on all computers
9. Business center computers do not require passwords
10. She was able to access the hotel's wireless from across the street

After receiving the list, the owners told Julie that a competing hotel a couple of blocks away just had their network hacked and were unsure of the damage. Since this was the fifth hotel in their area to be breached this week, they were worried that they might be next. They wanted her to act fast. Julie was by no means done with her audit and was sure that she would find many more points of vulnerability, but she believed that these were most of the "big ones." She knew that network security was both an art and a science, but she needed to start somewhere to secure the operation.

Learning Activity

1. What should Julie do first?
2. Why should she do this first?
3. List in order your next nine priorities and justify your answers.
4. Apart from these ten, can you think of other possible vulnerable points?

14. Key Terms

Attenuation
Bandwidth
Bluetooth
Botnet
Bottleneck
Cable Modems
Cellular
Channel
Client/Server (C/S)

Cloud Computing
Coaxial cable
Code Division Multiple Access (CDMA)
Convergence
Domain Name Server (DNS)
digital subscriber lines (DSL)
Electronic Data interchange (EDI)
Encryption
Extensible Markup Language (XML)
Firewall
Fiber Optics
File Transfer Protocol (FTP)
Gateway
Global Systems for Mobile communications (GSM)
Hypervisor
Link Load Balancer
Local Area Network (LAN)
Long-Term Evolution (LTE)
Modem
Near Field Communication (NFC)
Network Interface Card (NIC)
Network Operating System (NOS)
Network
Networking
Network Behavior Analysis (NBA)
Personal Communication Services (PCS)
Peer to Peer
Phishing
Port
Private Branch Exchange (PBX)
Router
Server
Social Engineering
Software as a Service (SaaS)
Spyware
Switch
T1
TCP/IP
Telecommunications
Trojan Horse
Twisted Pair
Utilities Fiber Network
Unified Communication
Uniform Resource Locator (URL)
Virtualization
Virtual Private Network (VPN)
Voice Over Internet protocol (VOIP)
Wireless Application Protocol (WAP)
Web Server
Wide Area Network (WAN)
WiMax
Wireless
Wireless Markup Language (WML)
World Wide Web
Worm

15. Chapter Questions

1. What is the difference between a router and a server?
2. Describe the different mediums used in data transmission.
3. What is the main difference between client/server and peer to peer networks?
4. What is an extranet and how can it be used advantageously in hospitality?
5. How is FTP used?
6. What is social engineering?
7. How can management make a network secure?
8. What is cloud computing?
9. What network issues should small organizations consider?
10. How is network understanding related to hospitality management?

16. References

Davidson, Johnathan, and Peters, James. (2000). *Voice over IP fundamentals.* Indianapolis: Cisco Press.

Laudon, Kenneth, and Laudon, Jane. 2009. *Management information systems* (8th ed.). Upper Saddle River, NJ: Prentice Hall.

Panko, Raymond R. 2007. *Business data networks and telecommunication* (6th ed.). Upper Saddle River, NJ: Prentice Hall.

Weisman, Carl J. 2000. *The essential guide to RF and wireless.* Upper Saddle River, NJ: Prentice Hall.

E-Commerce

Chapter Contents

INTERVIEW

Q: Hi Cindy, could you tell us a little bit about your background?

A: I have spent thirty years in hospitality and travel marketing. Most of the time was spent at the intersection of marketing and technology ranging from sales automation, reservation systems, distribution, online marketing, revenue management, data mining, and CRM. I worked for Hilton International for seven years heading up a new marketing information systems department and then moved into operations where I ended as a general manager for a four-hundred room full-service Hilton International hotel. I started my consulting practice in 1990 built on the marketing technology techniques I had developed, and in 1998 sold the business Driving Revenue to

Pegasus Solutions. I have since conducted research on an industry level examining best practices in distribution and online marketing for many sectors of the travel industry.

Q: How would you define e-commerce and online marketing?

A: E-commerce is a subset of the online marketing discipline that focuses on the booking component of the online experience. The travel marketer is now charged with a more comprehensive requirement for outreach so they can find and communicate to their consumers wherever they are browsing, gathering information, conversing, or buying online. The e-commerce piece is more directly related to the shopping and buying function.

Q: You know a lot about social networking. What are some of the keys to success for businesses engaging their customers through this medium?

A: Social networking is increasingly the way consumers are spending a portion of their time online. While some is purely social in nature where friends keep up with friends and family, much of it involves a method used for information collection. Typically, a consumer interested in a travel industry purchase would spend some time gathering information about options, pricing, and other factors depending on the nature of the purchase. There is a large percentage of consumers who will include one or more social networking sites as part of this process. They may use sites to read other consumers' reviews and to look at photos and videos of others' experience in a similar destination.

In terms of success in the use of social media and networks, a travel marketer needs to become immersed in the world in which his consumers reside. This will include reading the reviews they write, the blogs they respond to, and the commentary they make about different travel products and services. When there is a dialogue between consumers, there is a lot to gain for the astute marketer who wants to understand what drives the purchase and use of his products.

The main opportunities for the travel marketer are to listen, respond as needed and to provide and/or participate in forums to stimulate discussion on the topics about which the marketer wants to gain more intelligence or garner more attention.

Q: How about keys to success for Online Marketing in general?

A: Online marketing in general requires a shift in direction away from a focus on the marketer's own Web site with a push toward distributing content to all the Web sites where a consumer would go to find information about the marketer's products and services. It's not just getting things right on your Web site, which is still important, but the relevant content has to find its way to all the places consumers are browsing, info gathering, and shopping. "Distribution" is evolving from its original emphasis on reservations to a blend between message and booking distribution. It is incumbent upon the travel marketer to have an online presence at each point of contact with the consumer, and many of these points will not be on the marketer's own Web site. Learning how to manage this widespread presence is challenging because it is a complex network to master, and also because it is a dynamic environment that requires constant vigilance to know well enough to manage effectively.

Q: Looking into your crystal ball, any predictions as to how online marketing will continue to affect the hospitality industry?

A: The dominance of online marketing in the hospitality revenue toolkit will continue for some time. The marketer's drive to facilitate customer engagement will become the overarching strategic theme with the techniques for building traffic and bookings as the main part of the tactical plan.