9-1-2008

Hotel Network Security: A Study of Computer Networks in U.S. Hotels

Josh Ogle

Erica L. Wagner Ph.D.

Mark P. Talbert
Cornell University, mpt2@cornell.edu

Hotel Network Security: A Study of Computer Networks in U.S. Hotels

Abstract
A study of 147 U.S. hotels finds a mixed picture with regard to the security of guests' connections to the hotels' network, whether by cable or Wi-Fi. Since many business travelers connect remotely to continue working while on the road, the potential for theft of corporate information exists. Some hotels still rely on relatively rudimentary hub technology for their networks, and these are particularly subject to hacking. Others have upgraded to more secure switches or routers. Even better is encryption for Wi-Fi connections, but that still does not prevent malicious users from intercepting guests' transmissions. An example of a best practice is presented in the case of the W Dallas Hotel—Victory, which has set up virtual local area networks (VLANs) for all of its users. The VLAN inhibits attackers from using their computer to imitate the hotel's main server, which is the mechanism most would use to intercept other people's data. Given that the technology exists to increase a hotel network's security, a hotel could potentially be considered at fault for not taking the necessary precautions to protect their guests from hackers.

Keywords
hotels, computer networks, Wi-Fi, network security

Disciplines
Business | Hospitality Administration and Management

Comments

The Center for Hospitality Research
Hospitality Leadership Through Learning

Hotel Network Security: A Study of Computer Networks in U.S. Hotels

Cornell Hospitality Report
Vol. 8, No. 15, September 2008

by Josh Ogle, Erica Wagner, Ph.D., and Mark Talbert

Cornell University
School of Hotel Administration

The Robert A. and Jan M. Beck Center at Cornell University
Back cover photo by permission of *The Cornellian* and Jeff Wang.

Cornell Hospitality Report,
Volume 8, No. 15 (September 2008)
Single copy price US$50

Cornell Hospitality Report is produced for the benefit of the hospitality industry by The Center for Hospitality Research at Cornell University

David Sherwyn, *Academic Director*
Jennifer Macera, *Associate Director*
Glenn Withiam, *Director of Publications*

Center for Hospitality Research
Cornell University
School of Hotel Administration
537 Statler Hall
Ithaca, NY 14853

Phone: 607-255-9780
Fax: 607-254-2292
www.chr.cornell.edu

The Center for Hospitality Research

Hospitality Leadership Through Learning

Thank you to our generous Corporate Members

Senior Partners

American Airlines Admirals Club
General Growth Properties, Inc.
job.travel
Southern Wine and Spirits of New York
Taj Hotels Resorts Palaces
TIG Global LLC

Partners

AIG Global Real Estate Investment
Davis & Gilbert LLP
Deloitte & Touche USA LLP
Denihan Hospitality Group
Expedia, Inc.
Four Seasons Hotels and Resorts
Fox Rothschild LLP
FX Real Estate and Entertainment, Inc.
HVS
InterContinental Hotels Group
JohnsonDiversey
Jumeirah Group
LRP Publications
Marriott International, Inc.
Marsh's Hospitality Practice
Mobil Travel Guide
Nestlé
PricewaterhouseCoopers
Proskauer Rose LLP
Smith Travel Research
SynXis, a Sabre Holdings Company
Thayer Lodging Group
Travelport
WATG
WhiteSand Consulting

Friends

American Tescor, LLP • Argyle Executive Forum • Caribbean Hotel Restaurant Buyer's Guide • Cody Kramer Imports • Cruise Industry News • DK Shifflet & Associates • ehotelier.com • EyeforTravel • Fireman's Fund • 4Hoteliers.com • Gerencia de Hoteles & Restaurantes • Global Hospitality Resources • Hospitality Financial and Technological Professionals • hospitalityInside.com • hospitalitynet.org • Hospitality Technology • Hotel Asia Pacific • Hotel China • HotelExecutive.com • Hotel Interactive • Hotel Resource • International CHRIE • International Hotel and Restaurant Association • International Hotel Conference • International Society of Hospitality Consultants • iPerceptions • Lodging Hospitality • Lodging Magazine • Milestone Internet Marketing • MindFolio • Parasol • PKF Hospitality Research • RealShare Hotel Investment & Finance Summit • Resort+Recreation Magazine • The Resort Trades • RestaurantEdge.com • Shibata Publishing Co. • Synovate • The Lodging Conference • TravelCLICK • UniFocus • WageWatch, Inc. • WIWIH.COM

Cornell University
School of Hotel Administration

Hotel Network Security:

A Study of the Computer Networks in U.S. Hotels

by Josh Ogle, Erica L. Wagner, and Mark P. Talbert

EXECUTIVE SUMMARY

A study of 147 U.S. hotels finds a mixed picture with regard to the security of guests' connections to the hotels' network, whether by cable or wi-fi. Since many business travelers connect remotely to continue working while on the road, the potential for theft of corporate information exists. Some hotels still rely on relatively rudimentary hub technology for their networks, and these are particularly subject to hacking. Others have upgraded to more secure switches or routers. Even better is encryption for wi-fi connections, but that still does not prevent malicious users from intercepting guests' transmissions. An example of a best practice is presented in the case of the W Dallas Hotel–Victory, which has set up virtual local area networks (VLANs) for all of its users. The VLAN inhibits attackers from using their computer to imitate the hotel's main server, which is the mechanism most would use to intercept other people's data. Given that the technology exists to increase a hotel network's security, a hotel could potentially be considered at fault for not taking the necessary precautions to protect their guests from hackers.

ABOUT THE AUTHORS

A graduate of the Cornell University School of Hotel Administration, **Josh Ogle** is president of TriVesta LLC, which provides information technology services to businesses (jogle@cornell.edu).

Erica Wagner, Ph.D., is an assistant professor at the School of Hotel Administration (elw32@cornell.edu). Specializing in the study of how newly introduced information technology is "made to work" within organizations, she is particularly interested in how new technology can be accepted within organizations even when it is perceived as problematic, and the role played by the "best practices" concept. She has published widely in both scholarly and applied outlets.

The holder of a Master in Professional Studies degree from Cornell University, **Mark P. Talbert** is a senior lecturer in the information technology area of the School of Hotel Administration (mpt2@cornell.edu). In addition to his teaching responsibilities, he is the author of several educational software programs, including the Competitive Hospitality Education Simulation Series, Yield Lab, and Menu Dynamics. An authority on real-time management simulation models, he has presented educational seminars to companies such as Inter-Continental Hotels, Group Accor, Holiday Inns Worldwide, Shangri-La, and the Peninsula Group.

Hotel Network Security:

A Study of Computer Networks in U.S. Hotels

by Josh Ogle, Erica L. Wagner, and Mark P. Talbert

The security of hotel guests' communications is of utmost importance. Sometimes, the choice of which hotel to use is made on the basis of security and privacy.[1] However, as we explain in this report, many hotels have flaws in their network topology that allow for exploitation by malicious users, thereby resulting in the loss of privacy for guests. In particular, we discuss the results of a survey which found that about one hotel in five still uses an antiquated hub-based network, a type of arrangement that is inherently flawed in terms of security. Similarly, hotels are providing unsecured wireless (wi-fi) connections that are not encrypted and are subject to hacking.

[1] *Joker*, retrieved March 10, 2008, from Joker.be, www.joker.be/En.Content.470.aspx.

All of this should ethically be enough of a reason for a hotel to invest in secure, properly implemented networks for guest use. More pragmatically, it could potentially be devastating to a hotel's reputation (as well as bottom line) were there ever a lawsuit brought against it for leaking guest data because of a network's insecurity. Taking this into consideration, we set out to study the extent to which such a threat exists. We conducted surveys, on-site testing, and interviews to gather information. Our study presents recommendations to hotels to protect the hotel or its network users. This includes recommending changes that would protect their guests' wi-fi transmissions. We conclude our report by offering a case study of the W Dallas hotel, which we consider to be an example of best practices in hotel network security through its use of virtual local area networks (VLANs). We also offer checklists for hoteliers interested in improving the security of their guest networks.

Background

Business travelers have become accustomed to remaining in touch on the road by finding internet hotspots, whether in a coffee shop or their hotel. The problem with such remote access is that the travelers and their companies often overlook the potential security implications of having their data thus exposed.

Not all companies have ignored this issue, and many have begun to implement security measures.[2] We note, however, that the approach used (typically, requiring valid login and password combinations) is hardly ever sufficient to stop would-be hackers, unless this arrangement is carefully implemented. The weakness is that the company does not control the remote link—that is, the hotel's network. This is an oft-overlooked reality that is the basis of many cases of corporate data theft.

Wired Networks

Let's review the basis of Ethernet communications, to see where the weaknesses exist. We have compiled a glossary of technical terms for your reference, found on the next page. Ethernet, the networking technology that is now used by over 95 percent of all LANs in the world,[3] was developed over thirty years ago by a research team led by Robert Metcalfe at Xerox's Palo Alto Research Center (PARC). Although it has seen revisions, the basic concept remains. In techspeak, it is described as a "multi-point data communication system with collision detection."[4] In normal language, Ethernet is used to connect computers together so that information can be exchanged. One of the best things about Ethernet is that it is reliable and has proven itself to be the worthiest way of setting up a wired network. However, its age, combined with the assumptions made when it was conceived, has proven to be Ethernet's biggest weakness as well.

[2] See, for example: *Juniper Networks*, August 16, 2004, retrieved March 10, 2008, www.juniper.net/company/presscenter/pr/2004/pr-040816.html.

[3] N.S. Nath, *Yipes, Teragate Team on Ethernet WAN,* May 4, 2007, retrieved January 12, 2008, from internetcommunications.tmcnet.com/topics/enterprise/articles/6649-yipes-teragate-team-ethernet-wan.htm.

[4] Xerox, Inc. *United States Patent: 4063220,* December 13, 1977, retrieved January 6, 2008, from patft.uspto.gov/netacgi/nph-Parser?u=%2Fnetahtml%2Fsrchnum.htm&Sect1=PTO1&Sect2=HITOFF&p=1&r=1&l=50&f=G&d=PALL&s1=4063220.PN.&OS=PN/4063220&RS=PN/4063220.

Glossary

Address Resolution Protocol or *ARP*: The network protocol used to find a computer's MAC address. This is the way that each computer on a network knows which other computer it is talking to. It keeps a "routing table" which connects the IP address, which is used on the internet predominantly, and the MAC address of a computer, which is used on Ethernet and LANs.

Encryption: An unreadable, cryptographic set of information that was created in plain text. Encryption is used so that even if an attacker intercepts the information being sent over the network, that data thief will (in most circumstances) have no easy way to read that information.

Ethernet: In 1974, Robert Metcalfe and David Boggs of Xerox presented a draft proposal for a "multipoint data communication system with collision detection." This proposal was met with some resistence, but ultimately Xerox applied for and received a patent for this new way of communicating between computers. Over three decades later and only slightly modified, this is still the standard computer network used in almost every LAN in the world.

Hub: An inexpensive, unsophisticated device which simply forwards all information it gets on any of its ports to every computer on its network.

Internet Protocol or *IP*: An IP address is, in the simplest terms, the address of a computer on the internet. Each computer on the internet has its own specific IP address for each session or connection.

Local Area Network or *LAN*: Think of a LAN as a miniature internet, where computer connections are only made in a small geographic area like an office building or hotel.

MAC Address: A unique address that is assigned to each hardware device which connects to the internet. This is hard-coded—it never changes—unlike IP, which changes depending on where a person connects to the internet.

Packet: A small piece of data sent by one computer to another. Many packets are put together to form an entire product such as an email, web page, or other document.

Router: The most advanced (and most expensive) of the three types of network traffic control devices. These can be configured to filter certain types of traffic, to act as a firewall to protect users on its network, and to do an array of other advanced networking features.

Switch: A slightly more intelligent version of a hub which is able to differentiate which computer sent it data and, as such, to which computer it should send any related returned data.

Wireless LAN or *WLAN*: On the surface, this is the same thing as a regular LAN, only without wires.

Virtual LAN or *VLAN*: A local area network that is able to only see other computers on its network. While the computer and its traffic still flows onto the normal LAN, a computer on a VLAN can only see the traffic on its own VLAN, making it difficult for the computer to cause security disruptions by imitating a hub or server.

Virtual Private Network or VPN: This is a network that is processed inside of another network. A VPN connection may be made to a business's network, and all data passing over the VPN will be encapsulated in encrypted packets which travel over whatever connection the user is on. So, by having this extra encapsulation and tunneling, it makes it impossible for someone to "sniff" the information being sent over a vulnerable network at a place such as a hotel.

When Ethernet was developed, computer costs were prohibitive and thereby limited mostly to company and university ownership. A key assumption in the protocol was that there would be no malicious users. Moreover, at its inception, Ethernet connected computers by cables. With few people connected, no one assumed there would be anyone but friends and co-workers connecting. With the lowering in cost of networking hardware, though, more and more companies began to use this excellent way of sharing information, and eventually the failure to authenticate users became a problem.

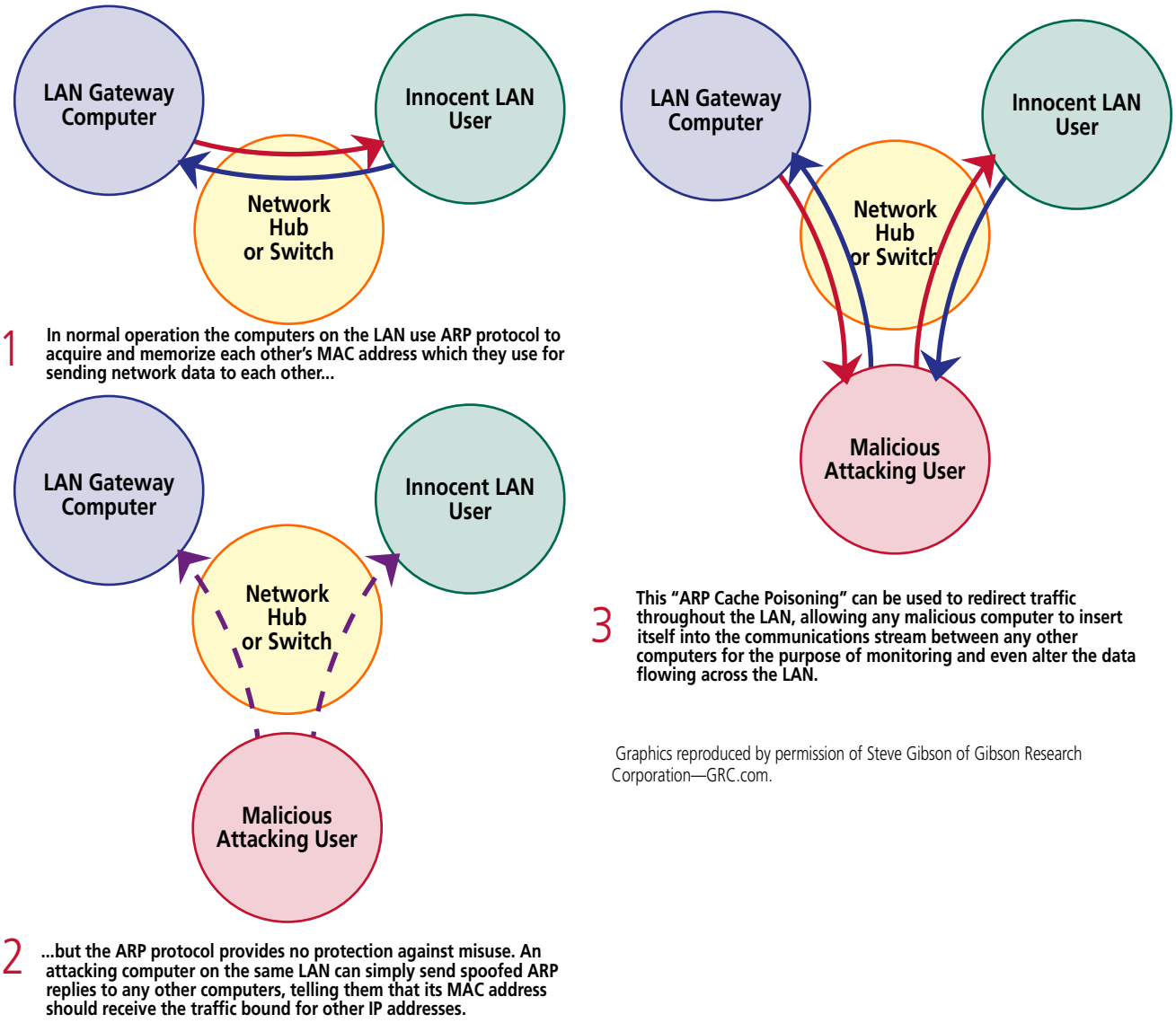
The flaws in Ethernet are easy to spot and difficult to overcome, even as access to the internet is fast becoming an expected amenity within the lodging industry. The best way to begin the analysis of how hotels can create relatively secure Ethernet services is with a basic understanding of the different possible types of networks. It is also worthwhile to note that having one type of system in your hotel does not preclude putting in another, different kind. In actuality, with a fairly competent IT staff, it could take as little as a couple of hours of switching out server hardware, and for minimal cost. The following are three basic ways to configure an Ethernet network.

Hubs

The most basic network configuration is to use a hub to handle traffic. This is the least expensive but also the least secure approach. As we indicated above, our research found that around 20 percent of the U.S. hotels we surveyed are using this antiquated, insecure network setup. As we discuss later, this issue could be fixed relatively easily.

The key problem with a hub is that it simply repeats any information that is sent to it. It has no built-in intelligence to know who sent what data, so to get the response packets (that is, computer data) back to the original sender, it re-transmits all packets to all users on the network. In an ideal situation, only the transmissions that are associated with your computer would come back to you. However, this is

Network Configurations—Authorized and Otherwise



Graphics reproduced by permission of Steve Gibson of Gibson Research Corporation—GRC.com.

impossible since the hub has no way of determining who on the network is sending what.

For example, if a guest in a hotel opened her web browser to www.cornell.edu on a hub-based network, the Cornell server would respond to the hotel's network and send the files needed to display Cornell's home page. These files would not only be sent to the person who requested the webpage, but would actually be sent out to every single person on that hotel's network. Most users would not receive this transmission because their computer is not automatically set up to receive other peoples' information, but any malicious user who wishes to illicitly receive these packets can do so by putting their network card into "promiscuous mode." With that setting, the promiscuous user can view all of the information that you, your friends, and anyone else connected to the network sends or receives—provided it is not encrypted. We emphasize that this eavesdropping really requires no competence on the part of the hacker, and requires no manipulation of the network. By their nature, hubs enable this type of environment.

Switches and Routers

One downside of hub-based networks, since all data are being re-transmitted to everyone on the network, is considerable congestion. Switches were developed in response to this congestion. A switch is a semi-intelligent device, slightly

We concluded that hotels in the U.S. are generally ill-prepared to protect their guests from network security issues.

more expensive than a hub, that is better than a hub at limiting collisions on an Ethernet network. It does so by learning the media access control (MAC) addresses of those who are sending data through it, and storing this information in its memory. Each MAC address on the network is assigned a physical port on the switch, so data come and go only to the MAC address with which the information is associated.

Routers work much the same way, but with the additional abilities to "hide" computers behind it, to route traffic in pre-programmed directions, and to act as a firewall to keep out unauthorized users. These added capabilities make the routers themselves more expensive than switches, though the benefits and flexibility gained from having routers implemented makes it well worth the slight increase in cost. Even after spending the extra money, though, there are still problems on the network that need to be addressed.

Both routers and switches are vulnerable to address resolution protocol (ARP) spoofing, which takes advantage of how Ethernet networks operate. ARP spoofing is depicted in the illustrations on the previous page. Most computers' network cards are set up to accept information in only two circumstances: **(1)** when data are sent directly to them and they are expecting it, and **(2)** when data are sent from what is called the broadcast address, which is a MAC address that is used by the router to help systems on a network find out what other computers are connected.

This arrangement uses the address resolution protocol, as follows. When you connect to an in-room computer port, it is common for your network card to send out a request to the router asking the addresses of all computers connected, and (if all is well) the computers on the network then respond with their addresses. This process forces the router to act like a hub, which opens up the door for a potential attacker to do damage.

The potential for exploitation occurs because this process makes no provision for authentication of the devices on the network. That is, there is no way to determine whether a particular user is legitimate. So, what an attacker will do is send an ARP reply to any other computer on the network, telling that computer that the attacker's computer is actually the gateway computer's MAC address. Since no verification is needed—all computers on the network trust each other—the victim's computer updates its ARP table with the attacker's information, and from then on all data that are sent out of the victim's computer go to the attacker's computer before going to the real gateway, which is the computer connecting the hotel's network to the internet.

After this happens, the attacker would then notify the router that his computer is the victim's computer, so now when any information is sent back to the victim's computer, it first goes through the attacker's. By doing this sequence, the attack will have successfully set up a "man-in-the-middle" attack, more specifically known in this case as ARP spoofing or ARP poisoning.

Though this process is technically complicated, tools freely available on the internet automate these tasks. It takes only five minutes to set up an attack, and the victim never knows what is happening. So far, we've been discussing this process as it would occur on a totally wired network. Next, let's turn to wireless setups, which add another level of complications.

Wireless Networks

As we explain below, our research found that around 90 percent of hotels are now offering wireless network connections to guests and sometimes to the general public. This is probably fueled by the necessities of today's business and leisure travelers. Most wireless networks, whether in the home or business environment, operate under the standards known as IEEE 802.11, which is a generally accepted protocol for wireless devices. Wireless networks can be thought of as hub-based networks, just without wires. Thus, a wi-fi system has the same vulnerability as the old hub-based networks. With a wired network, a person at least has to be plugged into an Ethernet jack to cause trouble, but with a wireless network a person can simply sit in a car outside of a hotel and capture all of the information traveling over the network, and no one would ever be the wiser.

Beyond the dangers inherent in Ethernet connections, a wireless environment has the additional vulnerability of

a "rogue hotspot." Rogue hotspots are essentially a wireless network's version of ARP spoofing. While the actual details of the technical setup are different, the result is the same: someone unknowingly sends requests through another computer, all the while believing the connection to be authentic. Here's how a rogue hotspot works.

Most operating systems are set up to connect to an open wireless network if one is available. Oftentimes, these are legitimate connections set up by companies to allow free internet access. A rogue hotspot claims to be an open, free wireless network, often with an inviting name, such as "Free Airport Wi-Fi." When the unsuspecting user connects, the attacker either sits idly by to gather the information that the user attempts to send over the network, or establishes a legitimate connection to the internet and act just as the ARP spoofer would do on a wired network. This way the victim continues to use the rogue network and has no idea that any information is being intercepted. Fortunately, there are ways of alleviating the security concerns that we have discussed, as explained after we discuss our survey.

Methodology

Our study employed online surveys, passive on-site testing, and interviews to determine the existing network infrastructures of a broad range of hotels, as well as their collective and individual susceptibility to the weaknesses that we have outlined. The online survey was sent to opt-in recipients of the Cornell School of Hotel Administration's Center for Hospitality Research list. Of the 5,000 recipients of the survey, 147 responded in the 76-day period between March 5, 2007, and May 19, 2007, equating to a roughly 3-percent completion rate.

The survey was used in part to determine the hotels' security arrangements (e.g., a router-based network topology, secured wireless access points, and limited-liability agreement notices to which users must agree) and whether these measures help prevent problematic situations (not to mention provide a defense in the case of litigation). The survey targeted IT professionals from a cross-section of hotel segments, including business hotels, family-oriented hotels, upper- and lower-scale hotels, and branded and independent hotels (see Exhibit 1, next page).

The results of this survey provided a foundation for our on-site tests, which involved visiting a total of forty-six hotels in the following eight cities: Arlington and Virginia Beach, Virginia; Charlotte and Raleigh, North Carolina; Dallas; Hagerstown, Maryland; Knoxville, Tennessee; and Pittsburgh.

You'll recognize that these eight cities are diverse, and each attracts a particular type of visitor. As a banking center, for instance, Charlotte attracts business and banking visitors, while Virginia Beach is a leisure destination. Hagerstown, in contrast, gets most of its traffic from the confluence of interstate highways. Consequently, we were able to gain a reasonable representation of the United States lodging market.

To test for possible weaknesses, co-author Josh Ogle brought along a laptop equipped with a modified version of the Linux operating system called BackTrack,[5] which is made specifically for penetration testing of networks. As a hacker might do, he also purchased a high-gain, omnidirectional antenna which hooked onto an SMC2532-B EliteConnect High Power wireless card to get better reception of the wireless networks' broadcasts. These were purchased at the suggestion of real hackers on an email list called "Full-Disclosure."[6]

Logging onto hotels' wireless networks was never a challenge. First, Ogle simply sat down in the lounge with a laptop, started BackTrack, and attempted to connect to the network. In the rare case that the network required a password or any other method of authentication, he would simply request the access instructions from the hotel staff, who were always glad to oblige. After connecting, he would load a packet-capturing program called Ethereal,[7] and capture approximately 1,000 packets. If any of these packets were not

---

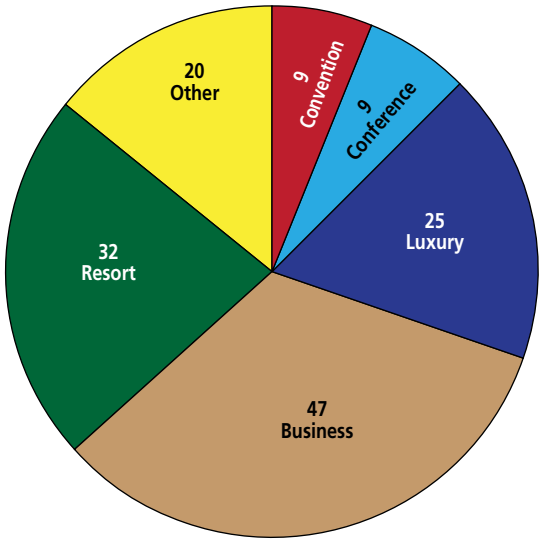
[5] *Remote-Exploit.org—Supplying Offensive Security Products to the World*, retrieved July 5, 2007, from www.remote-exploit.org/backtrack.html.

[6] *grok.org.uk/full-disclosure,* March 6, 2005, retrieved July 5, 2007, from www.grok.org.uk/full-disclosure/.

[7] *Ethereal: A Network Protocol Analyzer*, March 1, 2007, retrieved July 5, 2007, from www.ethereal.com/.

Exhibit 1

Types of hotel properties responding to the survey (147 properties)



normal "broadcast" packets (such as ARP, AppleTalk), and if he was able to see HTTP (website) or SMTP (email) traffic passing through, that meant the hotel had a vulnerable wireless setup. The process took about ten minutes per hotel, except for hotels that required authentication. That took a few more minutes and more assistance from hotel employees to breach.

Ogle checked in as a guest at eight hotels with wired networks, since that was the only way to gain network access. Once in the room, he would once again load up BackTrack and begin to analyze the network to see whether there were shared folders that were viewable, to see if he could break into the hotel's router (since the default password is rarely changed), and to see whether he could capture packets from other people's rooms by turning on the network card's promiscuous mode. As with the wireless tests, he recorded approximately 1,000 packets and ran these through Ethereal's filters to see whether there were any unauthorized types of traffic. If there were, it meant that the hotel's wired network was likely using a hub, rather than a more secure router or switch.

As a final step, Ogle visited the "W Dallas–Victory" hotel, to interview Domenic Carmona, the director of IT, so that the researchers could learn about industry best practices and to understand the costs (in both time and money) in setting up a properly secured network. We also wanted to find out first-hand what the threats were to network security in hotels. In addition, we wanted to find out whether the forward thinking of Carmona's particular hotel was by his own endeavor, or whether Starwood Hotels and Resorts (the national chain which owns the W brand) was thinking seriously about the potential liabilities of having a vulnerable computer network.

Results

Combining all methods of research—surveys, on-site testing, and the interview—we concluded that hotels in the U.S. are generally ill-prepared to protect their guests from the security problems inherent in Ethernet. We were forced to conclude further that most hotels have installed an amenity that they may not be managing properly.

A Snapshot of the U.S. Hotel Network Setup

Our survey questions were as formal and non-biased as possible. Comprehensive data include information regarding types of hotels, types of networks offered, quantity and quality of IT employees, and network topology. The survey results give what we consider an accurate snapshot of the hotel industry at the time of the study. The 147 survey respondents represented diverse hotels, of which about two-thirds were branded (roughly reflecting the distribution of U.S. hotels).[8]

Our survey indicated that 78.9 percent of responding hotels offer wired internet access (and have done so for an average of three years), and 92.5 percent offer wireless access (for an average of 20 months, see Exhibits 2 and 3). The predominance of wireless networks demonstrates the demand, but the issue of ensuring security remains in question. To that point, only 20.6 percent of the hotels have had reports of wrongdoing on their computer networks in their current form.

Effective security requires only one strong IT employee, and it turned out that the median number of full-time, regular employees on the hotels' IT staff was one. There were virtually no part-time or temporary IT employees at any of the hotels. Just over one-third of the hotels reported that their IT employee had received no training at all before beginning work, while 18.2 percent of hotels required training to the point of certification in an IT-related field (Exhibit 4). The average percentage of the IT budget spent on security was 9.5 percent, though some hotels spent as much as 80 percent and others nothing (Exhibit 5). We take this as an indication of managers' lack of security consciousness.

---

[8] R. Swig, *Independent Hotels: The New Brand Alternative,* June 2000, retrieved March 10, 2008, from www.hotel-online.com/Trends/Swig/Swig_IndependentBrand.html.

Exhibit 2

Length of time hotels have offered wired internet connections

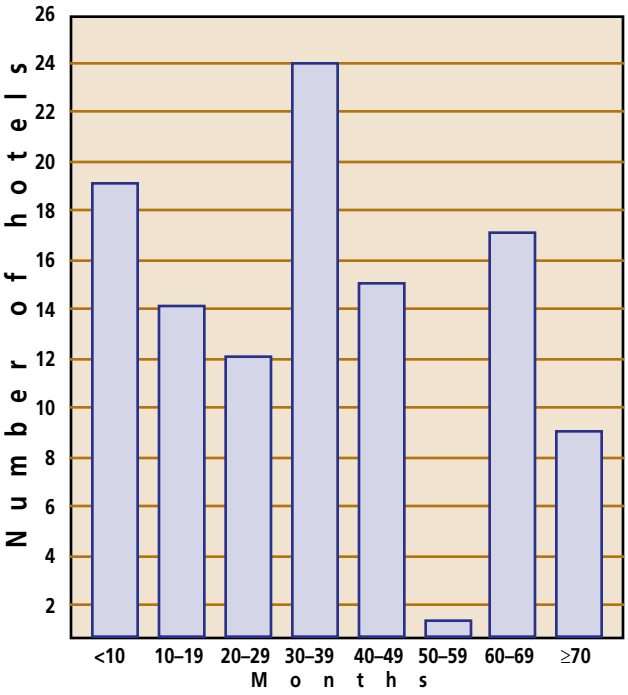


Exhibit 3

Length of time hotels have offered wireless internet connections

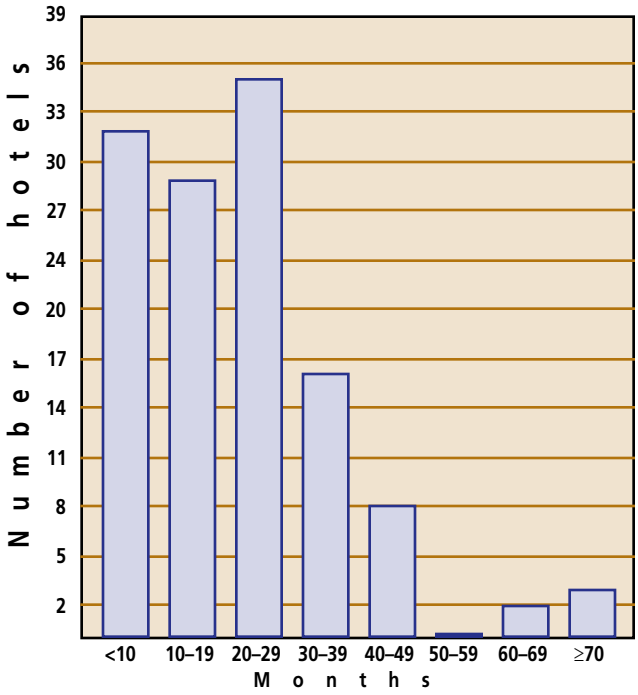
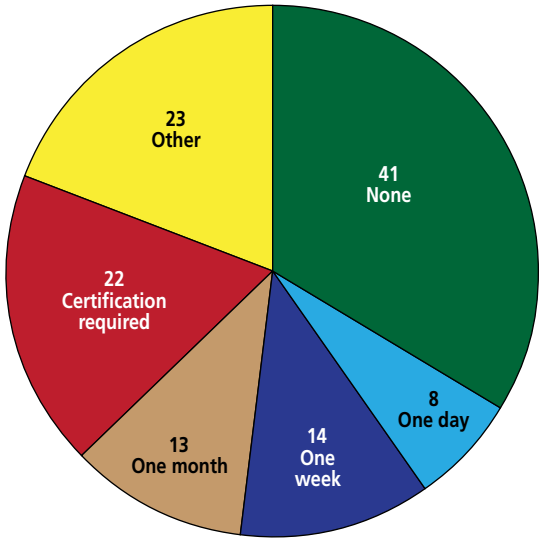


Exhibit 4

Length of training for hotel IT associates



Note: Graph numbers are based on a survey of 147 U.S. hotels. Not all hotels responded to all questions.

Exhibit 5

Percentage of IT budget spent on security

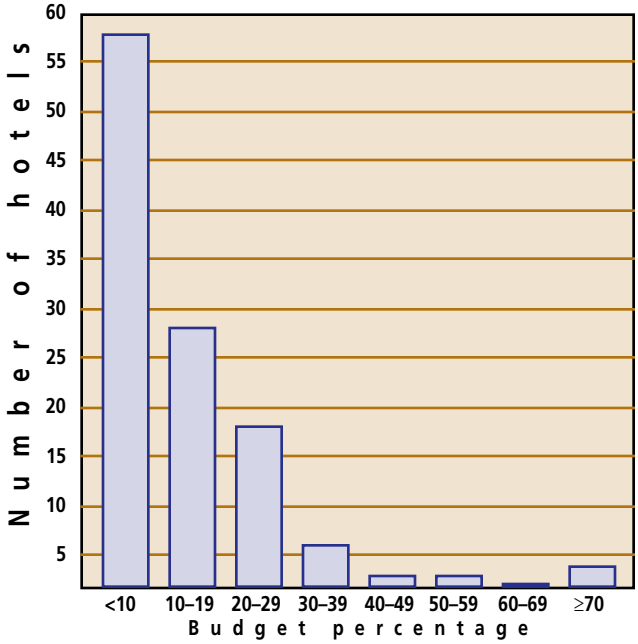
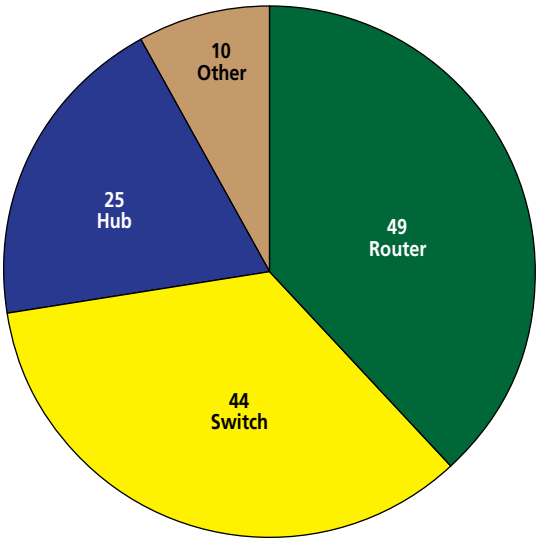


Exhibit 6

Hotels' network topology



Note: Graph numbers are based on a survey of 147 U.S. hotels. Not all hotels responded to all questions.

Looking at the hotels' network topology we found that a total of 72.7 percent used either router- or switch-based technology. However, 19.5 percent of the hotels had simple hub-based topology (Exhibit 6). In a wise approach, most of the hotels (82%) separated their own business's network from the one used by guests. The most secure way of doing this, by having two completely unassociated networks, was used by 63.6 percent of the respondents.

Security Check

As explained above, we collected data on forty-five hotels in eight cities. Of those tested, eleven were independent properties. All but one of the independent hotels offered wireless access, whereas twenty-nine of the thirty-four branded hotels offered wi-fi. This difference is not significant, given the small sample size, so for sake of the argument we will consider the two types of hotels to be equivalent in this regard.

Encryption. We found that encryption is not a widely used defense against network penetration. Just six of the thirty-nine wireless properties were using encryption. This is a meager outcome considering the importance of data protection. Four of the six hotels that used encryption also charged guests for use of their network. While this is a tiny sample, this might indicate that guests who pay for internet access get a better, safer experience. We'd like to think that the hotels use the revenue thus earned and put it into IT security, but we have no indication that this is the case.

Terms of service. One way to help a hotel's defense in the case of litigation regarding its insecure wireless network is to require guests to accede to a terms of service agreement. These typically have verbiage which indemnifies the hotel against future complaints arising out of any use of its network, including lost or stolen data. Five of the independent hotels and thirteen of the branded hotels used terms of service agreements. Interestingly, all six hotels that charged for the access enforced a terms of service agreement.

Best Practice Case Study: The W Dallas

Let's turn our focus to a hotel that we find epitomizes the properly implemented hotel network that is both accessible and secure, the W Dallas–Victory. Typical of most hotels, the W Dallas hotel has an IT staff of one, namely, Domenic Carmona, director of information technologies. He has been the architect of the hotel's network, which we found to be set up properly. The Dallas hotel's system is part of Starwood's initiative to keep guests' information safe, while maintaining easy access to the internet. Referring to Starwood, owner of the W Hotels brand, Carmona told us that "they really want to streamline the process but make it safe for the guest." He reiterated, "We like to keep everything streamlined and identify every device and node on our network and log traffic from each device."

One particular challenge for an IT team is to balance the twin goals of pleasing the guest and maintaining the network's safety. Forgetting this balance, network engi-

The wisest course for hotels is to secure their networks as much as possible, while still making them easy for guests to use.

neers sometimes set up barriers which hinder guests from enjoying their experience, and which require guests to jump through hoops and become a computer expert themselves just to read their email. Ease of use and security are not mutually exclusive, though, as. Carmona makes obvious in his use of Virtual LANs, or VLANs, on the network.

VLANs work by setting up an intranet, or internal network, which is physically attached to the rest of the network. The difference in a VLAN and a regular Ethernet setup, however, is that a VLAN permits access only to those computers which are on your own intranet. Since no information coming out of another user's network passes by your computer, the possibility of capturing other peoples' information is eliminated. If one were to set up VLANs on all ports in the hotel—that is, to make every single room its own VLAN—the chances for ARP spoofing and other hacks are minimized. VLANs also give the hotel more control over use of the network: "I can shut you off, turn you on, and I can tell what kind of traffic is going over the network," Carmona points out. In short, with a VLAN the IT staff can easily remove the ability for a malicious user to get on the internet in a secure environment.

Needless to say, Carmona's business and guest networks are separated physically, both operating through secure routers and separated from the internet by firewalls, as well as WPA encryption. Users have to agree to the hotel's terms of service before using its network. We see little more that could be done to secure the hotel's network at this juncture. Consequently, we judge that Carmona and the W Dallas–Victory hotel are a model of excellence in how to properly implement a secure, usable, smooth, wired and wireless network in a hotel, one which protects the guests from intrusion and the hotel from liability.

Steve Gibson of Gibson Research Corporation,[9] one of the world's foremost leaders in computer security and host of the SecurityNow! Podcast, agreed that the VLAN is an effective security tool. He told us, "Virtual LAN technology is a terrific solution for any sort of shared and insecure network environment. This effectively constrains any 'attack' to within its own VLAN. So, if … every physical port in the hotel would be on its own VLAN, there would be no possibility for cross-port snooping, sniffing, ARP poisoning, etc."

Secure Your Network

Looking at the potential for hacking, we urge hotels to secure their networks from would-be attackers. Though we acknowledge that there will always be a way to take advantage of the network, the steps suggested in the checklist on the next page can help protect your hotel from intrusion. Also on the next page, we offer a checklist for hotel guests to consider when they use a hotel's network. Hoteliers might wish to distribute this list to their guests. ■

[9] S. Gibson, *GRC | ARP Cache Poisoning,* December 11, 2005, retrieved January 22, 2008, from www.grc.com/nat/arp.htm.

Network Security Checklist

- ❑ We are using a router or switch to manage our network traffic.
- ❑ Our hotel business and guest networks are separate—if not separated physically, at least by a strict software firewall.
- ❑ When guests sign on to our network, they are presented with a terms of service page that they must accept to progress to the internet. This terms of service document should explicitly limit the liability of the hotel for anything occurring on the network, whether internal or external.
- ❑ We have considered and weighed the possibilities of setting up a VLAN on our network.
- ❑ We have small but noticeable public warning signs that emphasizes that guests use the network at their own risk.
- ❑ We attempt to hire staff with applicable computer security certifications, or we help our IT staff gain certification during their time working at the hotel.
- ❑ We have a training program for all of our IT staff which emphasizes how important it is to protect the network from intruders, lest the company be held liable for any wrong-doing.
- ❑ Our wireless network is password protected and encrypted with the latest wireless standards; we do not use WEP to protect our wireless network, as it is considered futile in the security world.
- ❑ We do not block VPN traffic for our users. VPN ports are commonly used by business people, and it is virtually the only real, secure way a person can connect to a remote location. With this in mind, we strive to make sure all VPN ports and protocols are allowed through the network.
- ❑ We train our employees not to give out proprietary hotel network information to anyone who is not clearly authorized to have such information. In the case of questionable intent of the inquirer, our employees are instructed to contact a manager immediately.

Note: While following the above checklist will help to ensure the network is safe, it is also important that the guests themselves pay particular attention to security. With that in mind, the accompanying checklist can be distributed to guests or posted publicly to instruct users on ways to protect their data while traveling.

Simple Precautions that Guests Can Take to Protect Their Data

- ◆ Only send important information over the internet if you ascertain that the connection is secure. For browsing the web, make sure that the address in the address bar says "https://" rather than simply "http://". The extra "s" means there is a "secure socket layer" between your computer and the website, meaning all information traveling over the network is encrypted. If possible, set up your email client to allow you to send using secure sockets, also, as this will encrypt the email information and disable it from being sniffed by an intruder.
- ◆ Make sure that up-to-date personal firewall software is installed. In any situation where someone is on the same network as you, you are open to attacks which exploit common computer program vulnerabilities. Running a firewall will help prevent any intrusions.
- ◆ If it is possible, always use VPN connections when doing anything on the internet, especially if it involves sensitive data. If your company does not supply a VPN connection, use an online service such as http://www.hotspotvpn.com or http://www.publicvpn.com to create a secure connection.
- ◆ Never connect to any "ad-hoc" or "peer to peer" wireless networks. These are almost always attackers disguising themselves as legitimate access points.

The above list should help to protect a guest if the instructions are followed fully. That is not to say the hotel guests would then be totally invulnerable to data theft, but we believe that these steps are the best protocol available at this writing.

Cornell Hospitality Reports

Index

www.chr.cornell.edu

2008 Reports

2008 Hospitality Tools

2008 Industry Perspectives

2007 Reports

Cornell Hospitality Reports Index (continued)
www.chr.cornell.edu

Vol. 7, No. 9 Compendium 2007

Vol. 7, No. 8 The Effects of Organizational Standards and Support Functions on Guest Service and Guest Satisfaction in Restaurants, by Alex M. Susskind, Ph.D., K. Michele Kacmar, Ph.D., and Carl P. Borchgrevink, Ph.D.

Vol. 7, No. 7 Restaurant Capacity Effectiveness: Leaving Money on the Tables, by Gary M. Thompson, Ph.D.

Vol. 7, No. 6 Card-checks and Neutrality Agreements: How Hotel Unions Staged a Comeback in 2006, by David Sherwyn, J.D., and Zev J. Eigen, J.D.

Vol. 7, No. 5 Enhancing Formal Interpersonal Skills Training through Post-Training Supplements, by Michael J. Tews, Ph.D., and J. Bruce Tracey, Ph.D
.
Vol. 7, No. 4 Brand Segmentation in the Hotel and Cruise Industries: Fact or Fiction?, by Michael Lynn, Ph.D.

Vol. 7, No. 3 The Effects on Perceived Restaurant Expensiveness of Tipping and Its Alternatives, by Shuo Wang and Michael Lynn, Ph.D.

Vol. 7, No. 2 Unlocking the Secrets of Customers' Choices, by Rohit Verma, Ph.D.

Vol. 7, No. 1 The Mixed Motive Instruction in Employment Discrimination Cases: What Employers Need to Know, by David Sherwyn, J.D., Steven Carvell, Ph.D., and Joseph Baumgarten, J.D.

2007 Hospitality Tools

CHR Tool 10 Workforce Staffing Optimizer, by Gary M. Thompson, Ph.D.

CHR Tool 9 Developing Hospitality Managers' Intercultural Communication Abilities: The Cocktail Party Simulation, by Daphne Jameson, Ph.D.

2006 Reports

Vol. 6, No. 15 The Cost of Employee Turnover: When the Devil Is in the Details, by J. Bruce Tracey, Ph.D., and Timothy R. Hinkin, Ph.D.

Vol. 6, No. 14 An Examination of Guest Complaints and Complaint Communication Channels: The Medium Does Matter!, by Alex M. Susskind, Ph.D.

Vol. 6, No. 11 A New Method for Measuring Housekeeping Performance Consistency, by Michael C. Sturman, Ph.D.

Vol. 6, No. 10 Intellectual Capital: A Key Driver of Hotel Performance, by Linda Canina, Ph.D., Cathy A. Enz, Ph.D., and Kate Walsh, Ph.D.

Vol. 6, No. 9 Mandatory Arbitration: Why Alternative Dispute Resolution May Be the Most Equitable Way to Resolve Discrimination Claims, by David Sherwyn, J.D.

Vol. 6, No. 8 Revenue Management in U.S. Hotels: 2001–2005, by Linda Canina, Ph.D., and Cathy A. Enz, Ph.D.

Vol. 6, No. 7 The Strategic Value of Information: A Manager's Guide to Profiting from Information Systems, by Gabriele Piccoli, Ph.D., and Paolo Torchio

CHR Tool 8 A Comprehensive Guide to Merchandising Bed and Breakfast Inns, by William J. Carroll, Ph.D., Betsy Gomez, Anna Huen, Pamela Lanier, and Iris Lui

Vol. 6, No. 6 Development and Use of a Web-based Tool to Measure the Costs of Employee Turnover: Preliminary Findings, by Timothy R. Hinkin, Ph.D., and J. Bruce Tracey, Ph.D.

Vol. 6, No. 5 Tipping and Its Alternatives: A Comparison of Tipping, Service Charges, and Service-inclusive Pricing, by Michael Lynn, Ph.D.

Vol. 6, No. 4 An Examination of Internet Intermediaries and Hotel Loyalty Programs: How Will Guests Get their Points?, by Bill Carroll, Ph.D., and Judy A. Siguaw, D.B.A

CHR Tool 7 A Picture Is Worth a Thousand Words: Using Photo-Elicitation to Solicit Hotel Guest Feedback, by Madeleine Pullman, Ph.D., and Stephani Robson

Vol. 6, No. 3 Compendium 2006

Vol. 6, No. 2 Why Discounting Still Doesn't Work: A Hotel Pricing Update, by Linda Canina, Ph.D. and Cathy A. Enz, Ph.D.

The Executive Path

Hospitality Leadership Through Learning

Cornell Short Courses and Certifications for Hotel Industry Professionals:

The General Managers Program

Tackle strategic hotel management issues and find relevant, specific solutions. Work with a global network of managers and top Cornell faculty in an intensive learning experience.

Ten-day programs are held on the Cornell University campus in Ithaca, New York in January and June and at the Cornell Nanyang Institute in Singapore in July-August.

Anheuser-Busch *The* Professional Development Program

Study and share experiences with peers from around the world in these intensive hospitality management seminars led by Cornell faculty and industry experts.

Intensive three-day courses are held on the Cornell University campus in Ithaca, New York in June-July; in Brussels, Belgium in June and at the Cornell Nanyang Institute in Singapore in January and July-August.

The Online Path

Available year-round, choose individual courses or combine courses to earn one of six Cornell Certificates. Interact with an expert instructor and a cohort of your peers to develop knowledge, and to effectively apply that knowledge in your organization.

The Contract Programs

Programs delivered by Cornell faculty for your company. Many hotel and foodservice management topics available, both "off the shelf" and custom developed to your needs and delivered to your management team on the Cornell campus or anywhere in the world.

Complete program information and applications online:

www.hotelschool.cornell.edu/execed/chr

PHONE: +1 607 255 4919 EMAIL: exec_ed_hotel@cornell.edu

Cornell University
School of Hotel Administration

www.chr.cornell.edu